

SPECTRUM[®]

Portable Management Application
for the
SEHI-22/24 and SEHI-32/34

User's Guide

CABLETRON
*SYSTEMS*_{Inc.}

The Complete Networking Solution

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 1996 by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9030954-E9 October 1996

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

SPECTRUM, **MiniMMAC**, **FNB**, **Multi Media Access Center**, and **DNI** are registered trademarks, and **Portable Management Application**, **IRM**, **IRM2**, **IRM3**, **IRBM**, **ESXMIM**, **ETSMIM**, **EMME**, **EMM-E6**, **ETWMIM**, **FDMMIM**, **FDCMIM**, **MicroMMAC**, **MRXI**, **MRXI-24**, **NB20E**, **NB25E**, **NB30**, **NB35E**, **NBR-620**, **SEHI**, **TRBMIM**, **TRMM**, **TRMM-2**, **TRMM-4**, **TRMMIM**, **TRXI**, **Media Interface Module**, **MIM**, and **Flexible Network Bus** are trademarks of Cabletron Systems, Inc.

UNIX and **OPENLOOK** are trademarks of Unix System Laboratories, Inc. **OSF/Motif** and **Motif** are trademarks of the Open Software Foundation, Inc. **X Window System** is a trademark of X Consortium, Inc. **Ethernet** and **XNS** are trademarks of Xerox Corporation. **Apple** and **AppleTalk** are registered trademarks of Apple Computer, Inc. **Banyan** is a registered trademark of Banyan Systems, Inc. **DECnet** is a registered trademark of Digital Equipment Corporation. **Novell** is a registered trademark of Novell, Inc. **CompuServe** is a registered trademark of CompuServe. **Sun Microsystems** is a registered trademark, and **Sun**, **SunNet**, and **OpenWindows** are trademarks of Sun Microsystems, Inc.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.
 - (b) This computer software may be:
 - (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;
 - (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
 - (3) Reproduced for safekeeping (archives) or backup purposes;
 - (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;
 - (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and
 - (6) Used or copied for use in or transferred to a replacement computer.
 - (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.
 - (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.
 - (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Chapter 1 Introduction to SPMA for the SEHI-22/24 and SEHI-32/34

Using the SEHI User's Guide.....	1-1
What's NOT in the SEHI User's Guide . . .	1-3
Conventions.....	1-3
Screen Displays	1-3
Using the Mouse	1-5
Getting Help	1-6
SEHI Firmware.....	1-7

Chapter 2 Using the SEHI Hub View

Using the Hub View	2-1
Navigating Through the Hub View	2-2
Hub View Front Panel.....	2-2
Using the Mouse in the Hub View Ports Display	2-5
Hub View Port Color Codes.....	2-6
Monitoring Hub Performance.....	2-7
Port Display Form.....	2-8
Checking Device Status and Updating Front Panel Info	2-10
Checking Module Status.....	2-11
Checking Repeater Status	2-12
Checking Port Status	2-13
Checking Statistics	2-15
General/Error Statistics.....	2-16
The SEHI Error Priority Scheme.....	2-18
Protocols/Frames Statistics.....	2-19
Viewing the Port Source Address List	2-19
Managing the Hub	2-20
Setting the Polling Intervals	2-21
Enabling/Disabling Ports.....	2-22

Chapter 3 Link/Seg Traps

What is a Segmentation Trap?.....	3-1
What is a Link Trap?	3-2
Enabling and Disabling Link/Seg Traps	3-2
Configuring Link/Seg Traps for the Repeater.....	3-4
Viewing and Configuring Link/Seg Traps for Hub Modules.....	3-4

Viewing and Configuring Link/Seg Traps for Ports 3-5

Chapter 4 Repeater Redundancy

Setting Network Circuit Redundancy 4-1
 Configuring a Redundant Circuit 4-2
Monitoring Redundancy 4-5

Chapter 5 Source Addressing

Displaying the Source Address List 5-1
 Setting the Ageing Time 5-4
Setting the Hash Type 5-4
Locking Source Addresses 5-5
 Source Address Locking on Older Devices 5-6
Configuring Source Address Traps 5-7
 Device-level Traps 5-8
 Module- and Port-level Traps 5-8
Finding a Source Address 5-11

Chapter 6 Security

What is LANVIEWsecure? 6-2
 The Newest LANVIEWsecure Features 6-4
 Security on Non-LANVIEWsecure Hubs 6-5
Configuring Security 6-6
 Resetting Learned Addresses 6-10
 Tips for Successfully Implementing Eavesdropper Protection 6-11
Enabling Security and Traps 6-12
 Repeater-level Security and Traps 6-13
 Hub-level Security and Traps 6-14
 Port-level Security and Traps 6-15

Appendix A SEHI MIB Structure

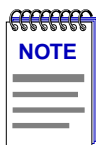
IETF MIB Support A-1
SEHI MIB Structure A-1
 A Brief Word About MIB Components and Community Names A-2

Index

Introduction to SPMA for the SEHI-22/24 and SEHI-32/34

How to use the SEHI User's Guide; manual conventions; contacting Cabletron Technical Support; SEHI firmware versions supported by SPMA

The SEHI-22/24 and SEHI-32/34 are intelligent repeating hubs that provide front panel ports for network connections and a rear-panel HUBStack Interconnect Bus port for stackable connections. Both devices fully conform to the IEEE 802.3 Repeater, AUI, and 10BASE-T specifications, and provide the flexibility to connect networks using a variety of media via RJ45 twisted pair, SMA and ST fiber optic, thin coax, and AUI EPIM modules. All of the models are functionally identical; the only difference among them is the configuration of front panel ports: the SEHI-22 has 12 built-in RJ45 ports and one slot for an EPIM module; the SEHI-24 has 24 built-in RJ45 ports and two EPIM slots; the SEHI-32 has one 50-pin Champ connector providing 12 twisted pair segments and one EPIM slot; and the SEHI-34 has two 50-pin Champ connectors providing 24 twisted pair segments and two EPIM slots. You can stack as many as four of Cabletron's SEH non-intelligent hubs with one SEHI and the entire stack is counted as only one repeater hop. All SEHI models will transmit re-timed data packets, regenerate preamble, extend fragments, arbitrate collisions, and automatically partition problem segments.



*Since the devices covered by this **User's Guide** are functionally identical, they will be jointly referred to throughout the text as the SEHI. Likewise, since the only differences in the windows for each device will be the device name (SEHI-22, SEHI-24, etc.) and the number of ports displayed, only the SEHI-24 windows will be shown.*

Using the SEHI User's Guide

Your SPECTRUM Portable Management Application (SPMA) for the SEHI-22/24 and SEHI-32/34 consists of a number of different applications, each of which provides a portion of the overall management functionality. Each of these

applications can be accessed from the icon menu (if you are using a management platform) and from the command line (if you are running in stand-alone mode); in addition, several applications can also be accessed from within the Hub View, a graphical display of the SEHI and its ports.

The *SEHI User's Guide* describes how to use many of the applications included with the module; note that the instructions provided in this guide apply to the SEHI regardless of the operating system or management platform you are using. Instructions for launching each individual function from the command line (stand-alone mode) are also included in each chapter.

Following is a description of the applications described in this guide; while we provide as much background information as we can, we do assume that you're familiar with Ethernet networks and general network management concepts:

- Chapter 1, **Introduction to SPMA for the SEHI-22/24 and SEHI-32/34**, describes the *SEHI User's Guide* and the conventions used in this and other SPMA manuals, explains where to find information about the SEHI, and tells you how to contact Cabletron Systems Technical Support.
- Chapter 2, **Using the SEHI Hub View**, describes the visual display of the Hub and explains how to use the mouse within the Hub View; the operation of some basic functions available only from within the Hub View (changing the Hub View display, opening menus and windows, enabling and disabling ports, checking device and port status, and so on) are also described.
- Chapter 3, **Link/Seg Traps**, describes how to configure link and segmentation traps to suit your management needs. You can access the Link/Seg Traps application from the icon menu, the Hub View, or the command line.
- Chapter 4, **Redundancy**, describes how to configure redundant circuits to keep your network connections up and running in the event of a single port's failure. You can access the Redundancy application from the icon menu, the Hub View, or the command line.
- Chapter 5, **Source Address**, describes how to display the Source Address List, how to set the ageing time, and how to configure source address traps; it also discusses the effects of source address locking. You can access the Source Address application from the icon menu, the Hub View, or the command line.
- Chapter 6, **Security**, describes how to configure intruder protection for all MIMs installed in the SEHI-controlled hubstack, and how to configure eavesdropper protection for any installed *LANVIEWSECURE* hubs. You can access the Security application from the icon menu, the Hub View, or the command line.
- Appendix A, **SEHI MIB Components**, lists the IETF MIBs supported by the SEHI, and describes their arrangement in a series of MIB components. A description of the objects controlled by each component is also included.

What's NOT in the SEHI User's Guide . . .

The following standard SPMA tools are available through the SEHI module and are explained in the *SPECTRUM Portable Management Application Tools Guide*:

- Charts, Graphs and Meters
- MAC Address Locator
- Community Names
- MIB I, II
- MIBTree
- TFTP Download
- Trap Table

The Charts, Graphs and Meters application is accessible from the Hub View and the command line; the MAC Address Locator application is accessible from the platform console window Tools menu; the rest of the tool applications are available only from the icon menu or the command line.

Instructions on discovering Cabletron devices, creating icons, and accessing the icon menus within your management platform are included in your *Installing and Using SPECTRUM for...* guide. If you are using SPMA for the SEHI in stand-alone mode — that is, without benefit of a specific network management system — instructions for starting each application from the command line are included in each chapter, both in this guide and in the *SPMA Tools Guide*.

Conventions

The family of SPECTRUM Portable Management Applications can work with a number of different network management systems running on several different operating systems and graphical user interfaces. This versatility presents two documentation problems: first, there is no standard terminology; and second, the appearance of the windows will differ based on the graphical interface in use. For the sake of consistency, the following conventions will be followed throughout this and other SPMA guides.

Screen Displays

SPMA runs under a variety of different operating systems and graphical user interfaces. To maintain a consistent presentation, screen displays in this and other SPMA guides show an OSF/Motif environment. If you're used to a different GUI, don't worry; the differences are minor. Buttons, boxes, borders, and menus displayed on your screen may look a bit different from what you see in the guide, but they're organized and labelled the same, located in the same places, and perform the same functions in all screen environments.

Some windows within SPMA applications can be re-sized; those windows will display the standard window resizing handles employed by your windowing system. Re-sizing a window doesn't re-size the information in the window; it just changes the amount of information that can be displayed (see Figure 1-1). When you shrink a window, scroll bars will appear as necessary so that you can scroll to view all the information that is available.

Cabletron Systems, Inc. EMME : 134.141.59.200							
8	7	6	5	4	3	2	1
ESX	TP-T	TPR-36	TP-32	SNAC	TPR-20	TPR-33	EMME
A	A	---	A	---	---	B	
Admin/Link	Admin/Link	No Mgt	Admin/Link	No Mgt	Admin/Link	Admin/Link	BDG Port Status
1 ON	1 NLK	1 SPEC	1 NLK	1 SPEC	1 ---	1 ON	
	2 NLK		2 NLK		2 NLK	2 NLK	A ON
	3 NLK		3 NLK		3 NLK	3 NLK	B ON
	4 NLK		4 NLK		4 NLK	4 NLK	C ON
	5 NLK		5 NLK		5 NLK	5 NLK	D ON
	6 NLK		6 NLK		6 NLK	6 NLK	BDG Port State
	7 NLK		7 NLK		7 NLK	7 NLK	
	8 NLK		8 NLK		8 NLK	8 NLK	A FWD
	9 NLK		9 NLK		9 NLK	9 NLK	B FWD
	10 NLK		10 NLK		10 NLK	10 NLK	C FWD
	11 NLK		11 NLK			11 NLK	D FWD
	12 NLK		12 NLK			12 NLK	AUI Redund
						13 NLK	
							1 DIS
							2 DIS

No Write Access to Device

History

Use the scroll bars provided to choose what to display in a window that's been resized.

Click here to display footer message history.

Figure 1-1. Window Conventions

Some windows will also contain a `History` button; selecting this button launches a History window (Figure 1-2) which lists all footer messages that have been displayed since the window was first invoked. This window can help you keep track of management actions you have taken since launching a management application.

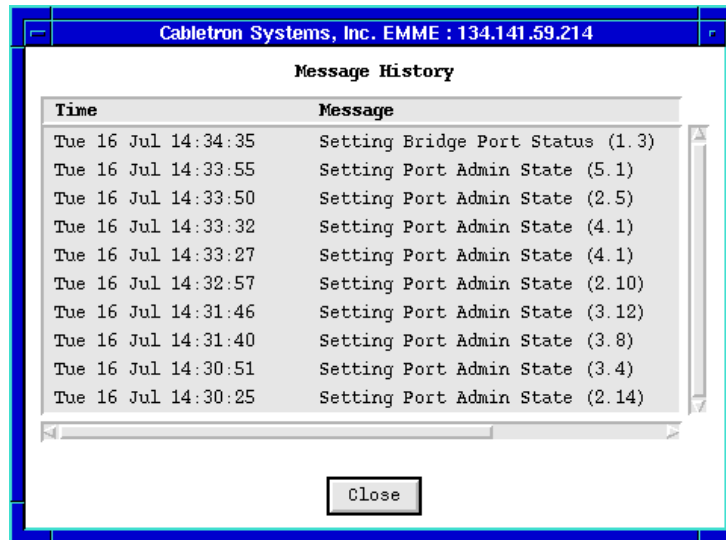


Figure 1-2. The History Window

Using the Mouse

The UNIX mouse has three buttons. Procedures within the SPMA document set refer to these buttons as follows:

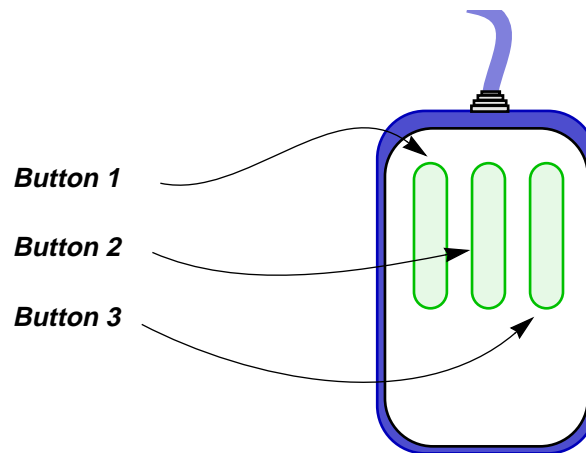


Figure 1-3. Mouse Buttons

If you're using a two-button mouse, don't worry. SPMA doesn't make use of mouse button 2. Just click the left button for button 1 and the right mouse button when instructed to use mouse button 3.

Whenever possible, we will instruct you on which mouse button to employ; however, menu buttons within SPMA applications will operate according to the convention employed by the active windowing system. By convention, menu buttons under the Motif windowing environment are activated by clicking the left mouse button (referred to as mouse button 1 in SPMA documentation), and there is no response to clicking the right button (mouse button 3). Under OpenWindows, menu buttons can be activated by clicking the right button, and convention dictates that the left button activates a default menu option; within SPMA, that default option will also display the entire menu. Because of this difference, references to activating a menu button will not include instructions about which mouse button to use. All other panels from which menus can be accessed, and all buttons which do not provide access to menus, will operate according to SPMA convention, as documented.

Getting Help

If you need additional support related to SPMA, or if you have any questions, comments, or suggestions related to this manual, contact Cabletron Systems Technical Support. Before calling, please have the following information ready:

- The product name and part number
- The version number of the program that you need help with. SPMA is modular, which means each application will have a specific revision number. Where applicable, an INFO button provides the version number; you can also view the version number for any application by typing the command to start the application followed by a `-v`.

You can contact Cabletron Systems Technical Support by any of the following methods:

By phone:	Monday through Friday between 8 AM and 8 PM Eastern Standard Time at (603) 332-9400.
By mail:	Cabletron Systems, Inc. PO Box 5005 Rochester, NH 03866-5005
By CompuServe [®] :	GO CTRON from any ! prompt
By Internet mail:	support@ctrn.com
FTP	ctrn.com (134.141.197.25)
Login	anonymous
Password	your email address
By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

For additional information about Cabletron Systems products, visit our World Wide Web site: <http://www.cabletron.com/>

SEHI Firmware

SPMA for the SEHI has been tested against firmware versions 1.10.04 and 1.05.03; if you have an earlier version of firmware and experience problems running SPMA contact Cabletron Systems Technical Support for upgrade information.

Using the SEHI Hub View

Navigating through the Hub View, monitoring hub performance; managing the hub

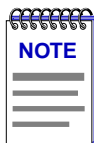
The heart of the SPECTRUM Portable Management Application (SPMA) for the SEHI is the Hub View, a graphical interface that gives you access to many of the functions that provide control over the device.

Using the Hub View

There are two ways to open the Hub View: if you are working within a network management system, you can select the **Hub View** option from the icon menu; specific directions for creating a SEHI icon and accessing the icon menu can be found in the appropriate *Installing and Using SPECTRUM for...* guide. If you are running the SEHI module in a stand-alone mode, type the following at the command line:

```
spmarun hubstack <IP address> <community name>
```

The community name you use to start the module must have at least **Read** access; for full management functionality, you should use a community name that provides **Read/Write** or **Superuser** access. For more information on community names, consult the appropriate *Installing and Using SPECTRUM for...* guide, and /or the **Community Names** chapter in the *SPMA Tools Guide*.

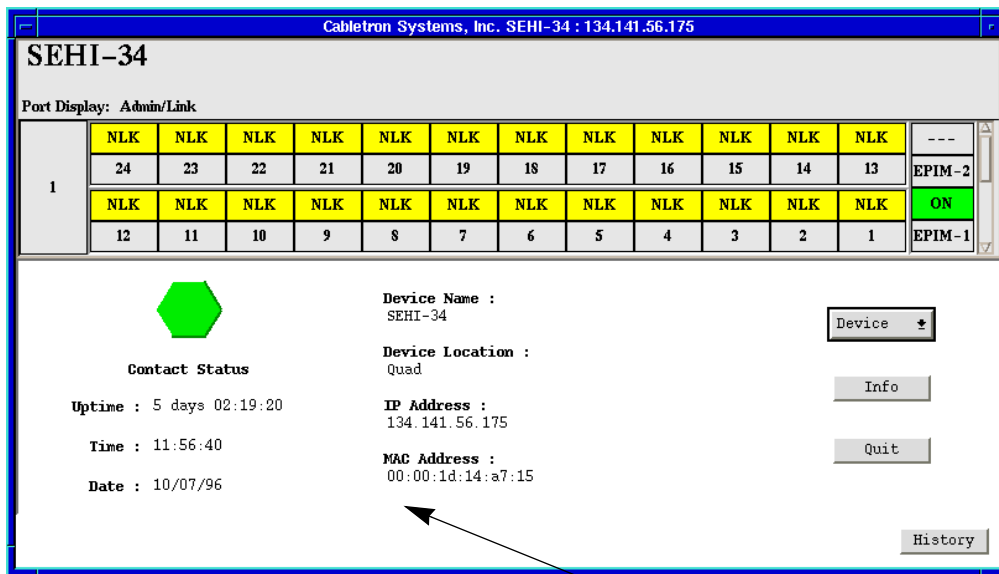


The `spmarun` script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.

*If there is a hostname mapped to your SEHI's IP address, you can use <hostname> in place of <IP address> to launch the Hub View. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

Navigating Through the Hub View

Within the Hub View (Figure 2-1), you can click mouse buttons in different areas of the window to access various menus and initiate certain management tasks. The following sections describe the information displayed in the Hub View Front Panel and how to use the mouse in the Hub View Ports Display.



Front Panel
Device summary information

Figure 2-1. SEHI Hub View

Hub View Front Panel

In addition to the graphical display of the modules, the Hub View gives you device level summary information. The following Front Panel information appears below the port display in the Hub View:



Contact Status is a color code that shows the status of the connection between SPMA and the device:

- Green means a valid connection.
- Blue means that SPMA is trying to reach the device but doesn't yet know if the connection will be successful.
- Red means that SPMA is unable to contact or has lost contact with the device.

Uptime

The time that the device has been running without interruption. The counter resets to 0 days 00:00:00 (X days HH:MM:SS) when one of the following occurs:

- Power to the device is cycled.
- The device is reset manually.

Date and Time

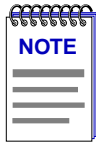
The date and time are taken from the device's internal clock.

Device Name

A text field that you can use to help identify the device.

Location

A text field that you can use to help identify the device.



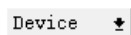
If you have assigned a device name or location that contains more than 19 characters, only the last 19 will be displayed in the Hub View. Check the Device Status window for the complete name and/or location, if necessary.

IP Address

The device's Internet Protocol address. You cannot change the SEHI's IP address from SPMA.

MAC Address

The device's factory-set hardware address. The MAC address cannot be changed.



Clicking on the **Device** button displays the Device menu, [Figure 2-2](#).

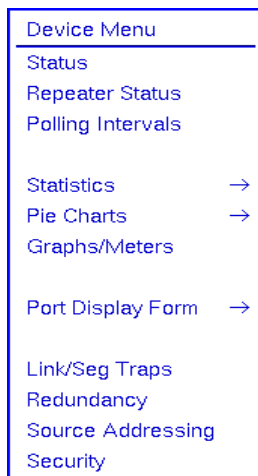


Figure 2-2. SEHI Hub View Device Menu

The Device menu lets you perform the following:

- Open the Device Status window
- Open the Repeater Status window
- Open the Polling Intervals window
- Open the Statistics windows
- Create device-level Pie Charts, Graphs and Meters
- Change the Port Display Form
- Launch the Link/Seg Traps application
- Launch the Redundancy application
- Launch the Source Addressing application
- Launch the Security application.

Note that the Device menu does not provide access to every application which is available to the SEHI; some information is only available from the Module or Port menus, and several applications can only be accessed either from the icon menu (if you are running under a network management platform) or from the command line (if you are running in stand-alone mode). See Chapter 1, **Introduction to SPMA for the SEHI-22/24 and SEHI-32/34**, for a complete list of applications available to the SEHI and how to access each one.

Info

If you need to call Cabletron's Technical Support about a problem with the Hub View application, you'll need the information provided in the Info window (Figure 2-3):

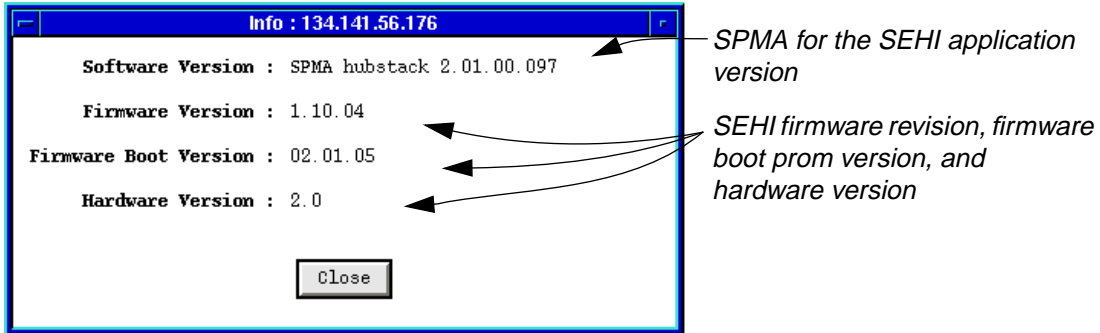


Figure 2-3. Hub Information Window

Quit

Clicking mouse button 1 on the **Quit** button closes all Hub View application windows; any open applications which can also be accessed from the command line or from the icon menu will remain open.

Using the Mouse in the Hub View Ports Display

Each device in your SEHI-managed HUBStack will have its own ports display in the Hub View; you can access the available ports displays by using the scroll bar located on the right side of the Hub View Ports Display window, as illustrated in Figure 2-4. The illustration below also indicates how to use the mouse to access the Module and Port menus and functions.

Port Display Form

Using the Module or Device menus, you can change the port display form shown in the Port Status boxes to any one of the following:

- Load (% of theoretical maximum)
- Traffic (Pkts/sec)
- Collisions (Colls/sec)
- Errors (Errors/sec, total or by type)
- Frame Sizes (% of total packets)

Port Status

The Port Status display changes with the type of port display format selected. Statistical selections display values in a statistic/second format. Load displays traffic as a percentage of theoretical maximum capacity. Port Type displays port status (ON, OFF, NLK, etc.). Click mouse button 1 to toggle the port between enabled and disabled; click mouse button 3 to display the Port menu.

Module Type

Displays the type of module, or device, whose ports are currently being displayed in the Ports Display.

SEHI-34

Port Display: Admin/Link

1	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	---
	24	23	22	21	20	19	18	17	16	15	14	13	EPIM-2
	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	NLK	ON
	12	11	10	9	8	7	6	5	4	3	2	1	EPIM-1

Module Index

Indicates the module's position in the SEHI-managed stack; the SEHI itself is always #1. Click mouse button 1 to open the Module Status window; click mouse button 3 to display the Module menu.

Port Index

Click mouse button 1 to open the Port Status window; click mouse button 3 to display the Port menu.

Scroll Bar

Use the scroll bar to rotate through the ports displays for each hub in the SEHI-managed stack.

Figure 2-4. Mousing Around a Ports Display

Hub View Port Color Codes

The Port Status boxes in the Hub View are color coded to indicate the port's connection status. The colors are consistent for all Port Display Forms except Admin Status; the exceptions are noted below.

- **Green** indicates that the port is active; that is, the port has been enabled by management, has a valid Link signal (if applicable), and is able to communicate with the station at the other end of the port's cable segment. Note that an AUI or transceiver port will display as active as long as it has been enabled by management, even if no cable is connected.

- **Blue** indicates that the port has been disabled through management.
- **Yellow** indicates that the port is enabled but does not currently have a valid connection. This usually indicates that the device at the other end of the segment is turned off.
- **Red** indicates that the port is enabled, but is not able to pass packets. This generally means that the port has been segmented by management after experiencing an excessive number of collisions; for a BNC (thin coax) port, however, this may only mean that no cable or terminator has been connected.

When the Admin Status port display option is active, only two colors apply: a port will be displayed in green if it is enabled by management, regardless of whether or not there is a cable attached or a valid link signal detected; a port disabled by management will display as blue.

Monitoring Hub Performance

The information displayed in the Hub View can give you a quick summary of device activity, status, and configuration. SPMA can also provide further details about device performance via its three-level menu structure. The Device, Module, and Port menus (Figure 2-5) give you control over the device at these three levels and give you access to the tools, menus, and windows that let you monitor specific aspects of device performance, change hub display options, and set SEHI operating and notification parameters. Remember, though many functions will operate the same at each level, those accessed via the Device menu control or provide information about the SEHI-managed stack as a whole; those accessed via the Module menu control or provide information about a single hub in the stack; and those accessed via the Port menu control or provide information about a single port.

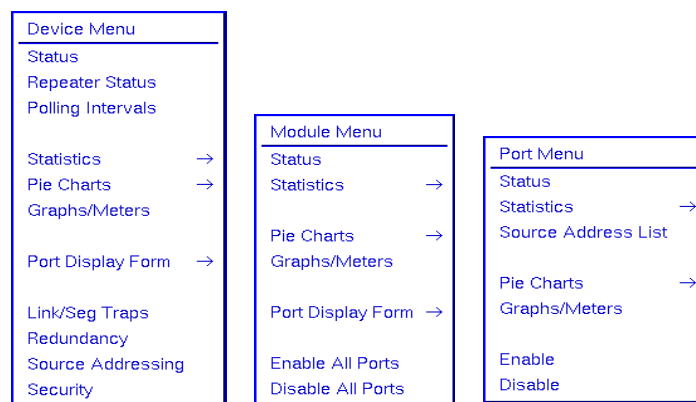


Figure 2-5. The SEHI's Device, Module, and Port Menus

Hub performance data available through these menus includes:

- Device, Module, and Port status descriptions.
- Device, Module, and Port statistics, which provide a complete breakdown of packet activity.
- Device, Module, and Port-level pie charts, graphs and meters, for a graphic representation of the types and levels of traffic passing through the device. (For more information about pie charts, graphs and meters, see the **Charts, Graphs and Meters** chapter in the *SPMA Tools Guide*.)

Port Display Form

You can change the type of information displayed for each port in the device by using the Port Display Form option on the Device and Module menus. Changing the port display form via the Device menu will affect all ports in the SEHI-controlled stack; changing the display form via the Module menu will affect only those ports on the selected device.

To change the port display form:

1. Click on the **Device** button to display the Device menu, or on the **Module Index** box to display the Module menu.
2. Drag down to **Port Display Form**, then right as necessary to select one of the port display options. The current selection will be displayed in the Port Display Form field on the port display.

Port display form options are:

Load

Shows a percentage for each active port that represents that port's portion of the theoretical maximum traffic level — for Ethernet networks, 10 megabits per second.

Collisions

Displays port traffic data in a collisions/second format. The SEHI counts both **receive** collisions — those collisions it detects while receiving a transmission — and **transmit** collisions — those it detects while transmitting (i.e., a port in the SEHI-managed stack transmitted one of the colliding packets); however, those counts are combined and a single total value is displayed.

Errors

Shows port traffic errors in an errors/second format. You can display any one of the following types of errors:

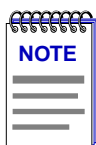
- Total errors
- Alignment errors
- CRC (Cyclic Redundancy Check) errors
- Runts
- Giants
- OOW (Out-of-Window) Collisions

For error type descriptions, see [Checking Statistics, page 2-15](#).

Frame Sizes

Displays a percentage for each active port that represents what portion of that port's traffic is of a specific size, measured in bytes. You can display any one of the following frame sizes:

- Runts (packets with fewer than 64 bytes)
- 64-127
- 128-255
- 256-511
- 512-1023
- 1024-1518
- Giants (packets with more than 1518 bytes)

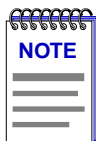


For the statistical port display form options listed above, three dashes (- - -) will display for all inactive ports; any active (green) port will display a numeric value, even if it's 0.0000.

Port Type

Provides the following administrative information about the port:

- **Admin/Link Status** indicates the connection status of the port:
 - ON indicates that the port has a valid link signal or does not support a link signal.
 - OFF indicates that the port has been turned off through management action.
 - NLK (No Link) indicates that the port does not have a link to a device at the other end of the cable, or that there is no cable attached.
 - SEG (Segmented) indicates that the port has been segmented by the repeater due to an excessive collision level.



Because BNC thin coax, AUI, and transceiver ports do not support the link feature, the displayed Admin/Link status for those ports may be misleading: for example, a BNC port will display as segmented when, in fact, there is no cable or terminator attached or the cable has been disconnected; an AUI or transceiver port will display as on (with a valid link signal) even when no cable is attached. Be sure to keep these anomalies in mind when troubleshooting a device so equipped.

- **Admin Status** displays either ON or OFF, an indication of whether management has the port enabled or disabled. A port can be ON but not operational; for example, under the Admin display, ports that are segmented or not linked are shown as ON.

- **Active Ports** displays either YES or NO for any active (green) port, indicating whether or not that port has seen any traffic at all since the device was last initialized or the counters were last reset; this port display form can tell you whether any port whose statistics are not currently incrementing has seen some activity in the past. Non-green (presumably inactive) ports will display three dashes (---), regardless of their past statistical activity.

Checking Device Status and Updating Front Panel Info

The Device Status window (Figure 2-6) is where you change the information displayed on the Hub View Front Panel and where you can see summary information about the current state of the device.

To open the Device Status window:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **Status** and release.



Figure 2-6. SEHI Device Status Window

Name and Location

These text fields help identify this SEHI-controlled HUBStack. The information you enter in the Name and Location boxes is written to the SEHI's MIB and appears on the Hub View front panel.

Contact

Use the Contact box to record the name and phone number of the person responsible for the device. Note that the information entered here is *not* displayed on the Hub View front panel.

Date and Time

Displays the current date and time from the SEHI's internal clock. Although the fields are static in the window, the front panel display is a real-time presentation.

To change the name, location, contact, date, or time:

1. Highlight the appropriate field and type the new values.
2. Press **Enter** or **Return** on the keyboard to save each change before moving on to another; each change will appear on the front panel as soon as **Enter** or **Return** is pressed.

Chassis Type

Displays the type of chassis used for the device (stand-alone).

Checking Module Status

You can open a Module Status window (Figure 2-7) for any device in the SEHI-controlled stack. To open the Module Status window:

1. Click mouse button 1 in the Module Index box. (Use the scroll bar to the right of the ports display to scroll through the available modules.)

or

1. Click mouse button 3 in the Module Index box to display the Module menu.
2. Drag down to **Status** and release.

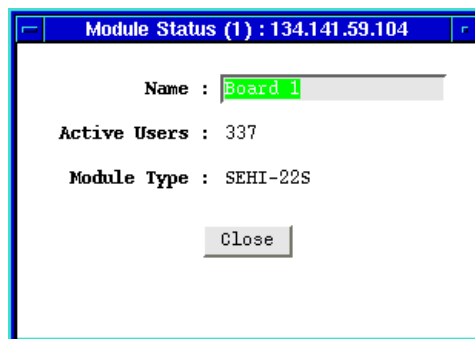


Figure 2-7. Module Status Window

Name

This text field can help identify the module, or device; the information entered here does not appear anywhere else in the Hub View.

To edit the Module Name:

1. Highlight the text in the Name box and type in a new name.

2. Press **Enter** or **Return** on the keyboard to save your changes.

Active Users

Displays the number of active source addresses communicating through this module.

Module Type

The type of module you are viewing (SEH- or SEHI-22, 24, 32, or 34).

Checking Repeater Status

The Repeater Status window (Figure 2-8) allows you to assign a name to the SEHI-controlled HUBStack as a whole. To open the Repeater Status window:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **Repeater Status** and release.

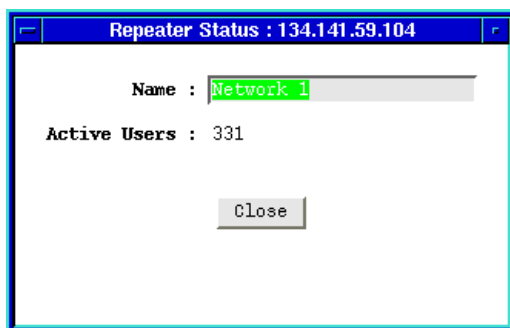


Figure 2-8. SEHI Repeater Status Window

Name

This field can help identify the SEHI-controlled stack as a whole; the information entered here is not displayed anywhere else in the Hub View.

To edit the Repeater Name:

1. Highlight the text in the Name box and type in a new name.
2. Press **Enter** or **Return** on the keyboard to save your changes.

Active Users

Displays the number of active source addresses communicating through this module.

Checking Port Status

You can open a Port Status window (Figure 2-9) for any port in the SEHI-controlled HUBStack. To open the Port Status window:

1. Click mouse button 1 in the **Port Index** box.
- or
1. Click mouse button 3 in the **Port Index** or **Port Status** box to display the Port menu.
 2. Drag down to **Status** and release.

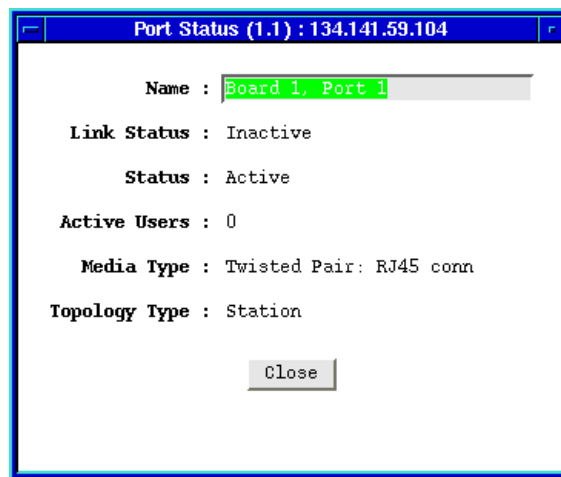


Figure 2-9. SEHI Port Status Window

Note that the window title includes the module and port number in parentheses; the rest of the window contains the following fields:

Name

This text field can help identify the port; the information entered here is not displayed anywhere else in the Hub View.

To edit the Name:

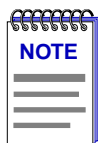
1. Highlight the text in the Name box and type in a new name.
2. Press **Enter** or **Return** on the keyboard to save your change.

Link Status

The port's Link Status tells you whether or not the port has a valid connection to the node at the other end of the cable segment. The possible Link conditions are:

- **Active** — The port has a valid connection with the device at the other end of the port's cable.

- **Inactive** — The device at the other end of the cable is turned off, there is a break in the cable, or there is no device or cable connected.
- **Not Supported** — The selected port does not support the Link feature, so the SEHI cannot determine link status; this value will show only for thin coax (BNC), AUI, or transceiver ports.



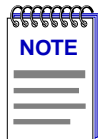
The fact that thin coax (BNC), AUI, and transceiver ports do not support the link feature can cause some misleading port status indicators: for example, a BNC port may show as segmented when, in fact, the cable has been disconnected; or an AUI or transceiver port may appear to have an active link when no cable has been attached. You should keep these anomalies in mind when troubleshooting a device so equipped.

- **Unknown** — The SEHI can't determine a link status.

Status

The port's Status can be one of three states:

- **Segmented**—A port becomes segmented (that is, disabled by the repeater module) when the port experiences 32 consecutive collisions, or when the port's collision detector is on for longer than approximately 2 to 3 milliseconds.



Because they do not support the link feature, thin coax (BNC) ports will display as segmented when there is no cable or terminator attached or the cable or terminator has been disconnected (i.e., a "no link" condition).

- **Active** —The port is operating normally.
- **Unknown** — The SEHI cannot determine port status.

Active Users

Each active source address communicating through the port is counted as an active user. If Active Users is greater than one, it indicates that the port is supporting a trunk connection.

Media Type

Indicates the type of cable segment connected to the port. The supported media types are:

- Twisted Pair: RJ45 conn(ector)
- BNC EPIM
- AUI EPIM
- Transceiver Port: AUI EPIM
- Twisted Pair: RJ45 EPIM
- Multi-Mode Fiber: SMA EPIM

- Multi-Mode Fiber: ST EPIM
- Single-Mode Fiber: ST EPIM

Topology Type

Indicates how the port is being used. The available types are:

- **Station**—The port is receiving packets from no devices, a single device, or two devices. Note that a port in station status may actually be connected to multiple devices; station status simply indicates that no more than two devices are currently active.
- **Trunk**—The port is receiving packets from three or more devices; it may be connected to a coax cable with multiple taps, or to a repeater or another MIM.
- **Unknown** — The SEHI cannot determine the topology status.

Checking Statistics

The Hub View can provide a summary of Ethernet statistics at the Device, Module, and Port levels, as shown in [Figure 2-10](#). The windows that display the statistics contain the same statistical categories at each level.

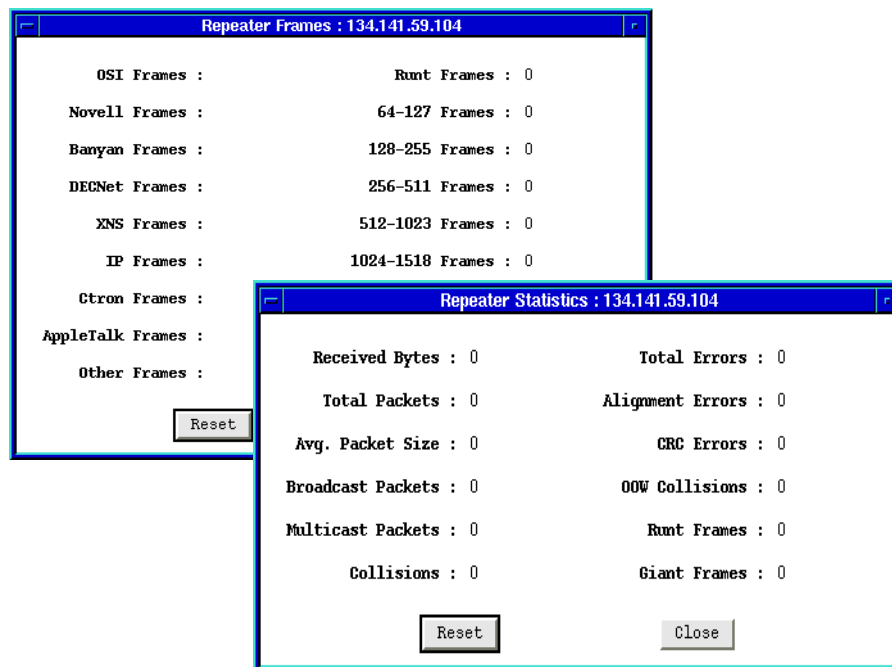
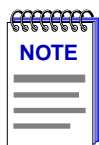


Figure 2-10. SEHI Statistics Windows (Device Level)

To view device statistics at the Device, Module, or Port levels:

1. Display the Device, Module, or Port menu by clicking mouse button 3 in the appropriate area (refer to [Figure 2-5, page 2-7](#)).
2. Drag down to **Statistics** and then right to either **General/Errors** or **Protocols/Frames** and release.

The Hub View begins counting the selected statistics when you open the window; counts will be cumulative until you use the **Reset** button or close the window.



When a device is reset, statistics windows and/or statistics displays in the Hub View may display very large numbers for one polling interval. This is due to the resetting of the counters.

Because the SEHI does not currently support Protocol counts, the Protocol fields in the Protocols/Frames window will remain blank.

Note that the module statistics windows include the module number in the window title; the port statistics windows include the module and port numbers in the window title.

General/Error Statistics

The General/Errors statistics windows display the following fields:

Received Bytes

The number of bytes of data received by this device, module, or port since the window was last opened or reset.

Total Packets

The number of packets of all types received by this device, module, or port since the window was last opened or reset.

Avg Packet Size

The number of bytes per packet received by this device, module, or port since the window was last opened or reset. The average packet size is calculated by dividing the number of bytes received by the number of packets received.

Broadcast Packets

The number of broadcast packets received by this device, module, or port since the window was last opened or reset. Broadcast packets have a single address recognized by each station on the net: this address is designated in IP form as 255.255.255.255, or in MAC hexadecimal form as FF-FF-FF-FF-FF-FF. The ARP and RARP requests sent by bridges and routers are broadcast packets.

Multicast Packets

The number of multicast packets received by this device, module, or port since the window was last opened or reset. Multicast packets are simultaneously addressed to more than one address, but fewer than all addresses.

Collisions

The number of collisions recorded by this device, module, or port since the window was last opened or reset. The SEHI counts both **receive** collisions — those detected while a port is receiving data — and **transmit** collisions — those detected while a port is transmitting data (i.e., the port has transmitted one of the colliding packets); however, these counts are combined and a single total value is displayed. Collisions of this type (called “legal” collisions, as opposed to the OOW collisions described below) are a natural by-product of a busy network; if you are experiencing high numbers of collisions, it may be time to redirect network traffic by using bridges or routers. Extremely high collision rates can also indicate a data loop (redundant connections) or a hardware problem (some station transmitting without listening first).

Total Errors

The number of errors of all types recorded by this device, module, or port since the window was last opened or reset.

Alignment Errors

The number of misaligned packets recorded since the window was last opened or reset. Misaligned packets are those which contain any unit of bits which is less than a byte — in other words, any group of bits fewer than 8. Misaligned packets can result from a packet formation problem, or from some cabling problem that is corrupting or losing data; they can also result from packets passing through more than two cascaded multi-port transceivers (a network design which does not meet accepted Ethernet spec).

CRC Errors

CRC, or Cyclic Redundancy Check, errors occur when packets are somehow damaged in transit. When each packet is transmitted, the transmitting device computes a frame check sequence (FCS) value based on the contents of the packet, and appends that value to the packet. The receiving station performs the same computation; if the FCS values differ, the packet is assumed to have been corrupted and is counted as a CRC error. CRC errors can result from a hardware problem causing an inaccurate computation of the FCS value, or from some other transmission problem that has garbled the original data. The CRC error counter shows the total number of CRC errors recorded since the window was last opened or reset.

OOW Collisions

The number of out-of-window collisions recorded since the window was last opened or reset. OOW collisions occur when a station receives a collision signal while still transmitting, but more than 51.2 μ sec (the maximum Ethernet propagation delay) after the transmission began. There are two conditions which can cause this type of error: either the network’s physical length exceeds IEEE

802.3 specifications, or a node on the net is transmitting without first listening for carrier sense (and beginning its illegal transmission more than 51.2 μ s after the first station began transmitting). Note that in both cases, the occurrence of the errors can be intermittent: in the case of excessive network length, OOW collisions will only occur when the farthest stations transmit at the same time; in the case of the node which is transmitting without listening, the malfunctioning node may only fail to listen occasionally, and not all of its failures to listen will result in OOW collisions — some may simply result in collisions (if the 51.2 μ s window has not yet closed), and some will get through fine (if no one else happens to be transmitting).

Runt Frames

The number of received packets smaller than the minimum Ethernet frame size of 64 bytes (excluding preamble). This minimum size is tied to the maximum propagation time of an Ethernet network segment — the maximum propagation time is 51.2 μ s, and it takes approximately 51.2 μ s to transmit 64 bytes of data; therefore, every node on the segment should be aware that another node is transmitting before the transmission is complete, providing for more accurate collision detection. Runts can sometimes result from collisions, and, as such, may be the natural by-product of a busy network; however, they can also indicate a hardware (packet formation), transmission (corrupted data), or network design (more than four cascaded repeaters) problem.

Giant Frames

The number of received packets that are longer than the maximum Ethernet size of 1518 bytes (excluding preamble). Giant packets typically occur when you have a jabbering node on your network — one that is continuously transmitting, or transmitting improperly for short bursts — probably due to a bad transmitter on the network interface card. Giant packets can also result from packets being corrupted as they are transmitted, either by the addition of garbage signal, or by the corruption of the bits that indicate frame size.

The SEHI Error Priority Scheme

Each Cabletron device employs an error priority scheme which determines how packets with multiple errors will be counted, and ensures that no error packet is counted more than once. The priority scheme for the SEHI counts errors in the following order:

1. OOW Collisions
2. Runts
3. Giants
4. Alignment Errors
5. CRC Errors

Knowing the priority scheme employed by the SEHI can tell you a lot about the error counts you are seeing. For example, you know that the number of packets

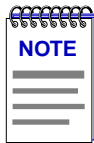
counted as CRC errors had *only* CRC errors — they were of legal size (not runts or giants) and had no truncated bytes. You also know that any packet less than 64 bytes long has been counted as a runt, even if it also had alignment and/or CRC problems (which is likely if the runt is the result of a collision or other transmission problem).

Protocols/Frames Statistics

The Protocols/Frames statistics windows display the following fields:

Protocols

- OSI Frames
- Novell Frames
- Banyan Frames
- DECNet Frames
- XNS (Xerox Network Systems) Frames
- IP Frames
- Ctron Frames
- AppleTalk Frames
- Other Frames



Because the SEHI does not currently support Protocol counts, the Protocol fields in the Protocols/Frames window will remain blank.

Frame Sizes

- Runt Frames (packets smaller than 64 bytes)
- 64-127 (byte) Frames
- 128-255 Frames
- 256-511 Frames
- 512-1023 Frames
- 1024-1518 Frames
- Giant Frames (packets larger than 1518 bytes)

Viewing the Port Source Address List

You can use the Source Address List option from the Port menu to view the Port Source Address List (Figure 2-11). The Port Source Address List contains the MAC address and its associated vendor name for each device communicating through a specific port on the SEHI or hubstack.

The full features of Source Addressing (including the device-level Source Address List, port locking, source address traps, and find source address) are discussed in the **Source Address** chapter, later in this book.

No.	MAC Address	Vendor
182	00:00:1D:03:2E:87	Cabletron
183	00:00:1D:0B:C2:C7	Cabletron
184	00:00:1D:05:6D:09	Cabletron
185	00:00:1D:08:98:25	Cabletron
186	00:00:1D:05:AA:C5	Cabletron
187	00:00:1D:05:62:AD	Cabletron
188	00:00:1D:09:59:D5	Cabletron
189	00:00:1D:0D:CC:B3	Cabletron
190	00:00:1D:07:9A:D0	Cabletron
191	00:00:1D:18:79:2A	Cabletron

Figure 2-11. The Port Source Address List

To view a port's Source Address List:

1. Display the Port menu by clicking mouse button 3 in the appropriate Port Status box.
2. Drag down to **Source Address List** and release.

The Source Address List window displays addresses of all devices that have transmitted packets that were detected by the selected port within a time period less than the Source Address Table's (SAT) defined ageing time (addresses that have not transmitted a packet during one complete cycle of the ageing timer will be purged). The Ageing Timer is user-configurable; see **Setting the Ageing Time** in the **Source Address** chapter, later in this manual. The List window can display about ten addresses at once; use the scroll bar to the right of the List window to view additional addresses, if necessary.

Since the SAT is constantly changing as old entries are aged out and new ones learned from the network, you should occasionally update a displayed list by clicking mouse button 1 on the button. Once displayed, the list is static and will not reflect recent changes. The displayed number of Active Users is also static; this field will also update when you click on .

Managing the Hub

In addition to the performance information described in the preceding sections, the Hub View also provides you with the tools you need to configure your HUBStack and keep it operating properly. Hub management functions include setting polling intervals, enabling ports at the module and port level, and disabling ports at the port level.

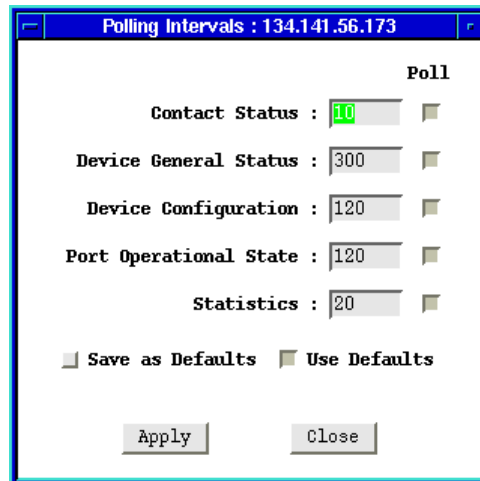


Figure 2-12. SEHI Polling Intervals

Setting the Polling Intervals

To set the polling intervals used by SPMA and the SEHI:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **Polling Intervals**, and release. The SEHI Polling Intervals window, [Figure 2-12](#), will appear.
3. To activate the desired polling, click mouse button 1 on the selection box to the right of each polling type field.
4. To change a polling interval, highlight the value you would like to change, and enter a new value in seconds. Note that the **Use Defaults** option must *not* be selected, or values will revert back to default levels when you click on **Apply**, and your changes will be ignored.
5. If you wish to use your new polling interval settings as the default values that SPMA will use for each SEHI-controlled stack you are managing, use mouse button 1 to select the **Save As Defaults** option.
6. If you wish to replace existing values with the current set of default values, use mouse button 1 to select the **Use Defaults** option.
7. Click mouse button 1 on the **Apply** button once your changes are complete. Changes take effect after the current polling cycle is complete.

You can set the update intervals for the following:

Contact Status

This polling interval controls how often the SEHI is “pinged” to check SPMA’s ability to maintain a connection with the device.

Device General Status

This polling interval controls how often the Hub View Front Panel Information — such as Uptime, Device Name, and so forth — and some port status information is updated.

Device Configuration

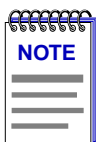
This polling interval controls how often a survey is conducted of the devices installed in your SEHI-controlled HUBStack.

Port Operational State

This polling interval controls the update of the information displayed in the Port Status boxes for each port in the device. Port state information includes link state (the color code) and admin state (on or off).

Statistics

This polling interval controls how often the information displayed in the Port Status boxes is updated when the Port Display Form is set to a rate or percentage, and how often the Device, Module, and Port statistics counts are updated.



SPMA generates network traffic when it retrieves the above-described information; keep in mind that shorter intervals mean increased network traffic. Range limits for these polling times are 0-999,999 seconds; however, an entry of 0 will be treated as a 1.

Enabling/Disabling Ports

You can enable and disable ports both from the Module menu, which affects all ports on a single module, or device; or from the Port menu, which affects individual ports.

To enable or disable an individual port:

1. Click mouse button 1 on the Port Status box to toggle the port On or Off.

or

1. Click mouse button 3 on the Port Index or Port Status box to display the Port menu.
2. Drag down to **Enable** or **Disable**, as appropriate, and release. The selected port changes color when its state changes. A disabled port is blue.

To enable or disable all ports in a module:

1. Click mouse button 3 on the Module Index box to open the Module menu.
2. Drag down to **Enable All Ports** or **Disable All Ports**, as appropriate, and release.

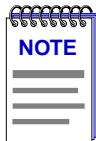


When disabling all ports on a module, make sure you don't disable the port through which your management station is communicating with the HUBStack, or you will lose contact with the stack.

Link/Seg Traps

What are Link and Segmentation traps; enabling and disabling these traps at the device, module, and port levels

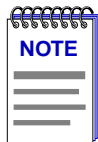
Among the traps which Cabletron devices are designed to generate are traps which indicate when a repeater port gains or loses a link signal, when the repeater segments (disconnects) a port due to collision activity, and when a segmented port becomes active again. In some networks, these Link and Segmentation traps may be more information than a network manager wants to see. So SPMA provides you with a means to selectively enable and disable Link and Segmentation traps: you can turn traps on and off for all ports on the SEHI, all ports on a selected module or modules, or for individual ports.



*SPMA does not accept the trap messages; that task is left to your network management system. (See the appropriate network management system documentation for details about viewing trap messages.) When this utility is used in stand-alone mode, traps will either be ignored when they return to the workstation from which you are running SPMA for the SEHI, or they will turn up at another management workstation which has been configured to accept traps. Note also that, regardless of the configuration performed using this utility, NO traps will be sent by the device unless its trap table has been properly configured; see the SEHI hardware manual and/or the **Trap Table** chapter in the **SPMA Tools Guide** for more information.*

What is a Segmentation Trap?

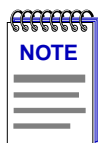
Cabletron's Ethernet repeaters count collisions at each port. If a port experiences 32 consecutive collisions, the repeater segments the port to isolate the source of the collisions from the rest of the network. When the repeater segments a port, it generates a **portSegmenting** trap. As soon as a segmented port receives a good packet, the repeater reconnects the port to the network and generates a **portUnsegmenting** trap.



Unterminated BNC (thin coax) ports appear in the Hub View as segmented ports. When you attach a thin coax cable or a 50 Ω terminator to a port, the repeater generates a **portUnsegmenting** trap; when you remove the cable or terminator, the repeater generates a **portSegmenting** trap. Note also that devices at both ends of the cable will generate the **portUnsegmenting** and **portSegmenting** traps, even if only one end of the cable has been disconnected.

What is a Link Trap?

Some Cabletron Ethernet repeater ports — including RJ45 twisted pair and fiber optic ports — generate a link signal to monitor the status of their connection with the device at the other end of the cable segment. If the cable is removed or broken, the port's link status goes to "No Link" and the repeater generates a **portLinkDown** trap. When a port in a "No Link" condition receives a link signal, the port goes to a "Link" condition and the repeater generates a **portLinkUp** trap. Note that devices at both ends of the disconnected or broken cable will generate the **portLinkDown** and **portLinkUp** traps, even when only one end of the cable has been removed.



BNC (thin coax), AUI, and transceiver ports do not support a link signal. As described above, BNC ports respond to changes in link status by generating **portSegmenting** and **portUnsegmenting** traps; AUI and transceiver ports do not respond at all to changes in link status (unless the port has been segmented due to excessive collisions), and will always display as on, even if no cable is connected.

Enabling and Disabling Link/Seg Traps

Although each Cabletron device comes with a number of traps built in to the firmware, no device will generate these traps unless it is configured to do so. This can be accomplished via Local Management (by enabling traps and entering your workstation's IP address in the Community Names screen), or via the SPMA Trap Table utility, accessible from the icon menu or from the command line. Once traps as a whole have been enabled, you can use the Link/Seg Traps feature to selectively enable and disable link and segmentation traps as required by your network management needs.

To open the Repeater Link/Seg Traps window:

from the icon:

1. Click on the appropriate SEHI icon to display the icon menu.
2. Drag down to **Link/Seg Traps** and release.

from the Hub View:

1. Click on `Device` to display the Device menu.
2. Drag down to **Link/Seg Traps** and release.

from the command line (stand-alone mode):

1. From the appropriate directory, type

```
spmarun r4hwtr <IP address> <community name>
```



The *spmarun* script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.

If you wish to change any Link/Seg Trap settings, be sure to use a **community name** with at least Read/Write access. If you only wish to view current settings, a community name with Read access will be sufficient.

If there is a hostname mapped to your SEHI's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.

The main Repeater Link/Seg Traps window, [Figure 3-1](#), will appear.

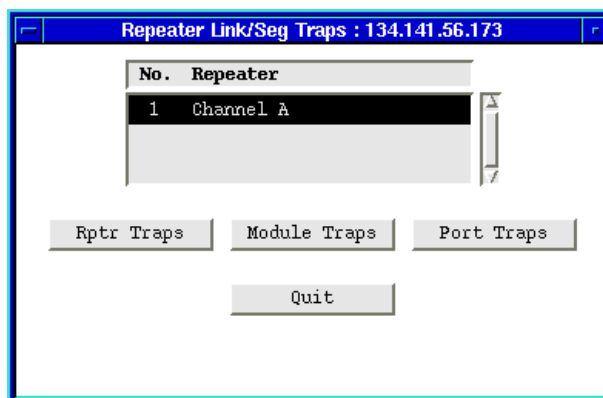


Figure 3-1. Repeater Link/Seg Traps Window

Configuring Link/Seg Traps for the Repeater

To enable or disable Link and Segmentation traps for all ports on a repeater:

1. In the Repeater Link/Seg Traps window, click mouse button 1 on the repeater interface for which you would like to configure link and segmentation traps.
2. Click mouse button 1 on ; the Channel X Link/Seg Traps window, [Figure 3-2](#), will appear.

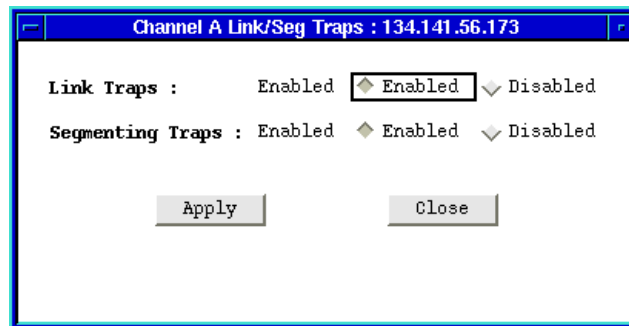


Figure 3-2. Channel X Link/Seg Traps Window

3. In the **Link Traps** field, click mouse button 1 on the appropriate selection to **Enable** or **Disable** link traps for the repeater.
4. In the **Segmenting Traps** field, click mouse button 1 on the appropriate selection to **Enable** or **Disable** segmenting traps for the repeater.
5. Click mouse button 1 on to save your changes; the current status will be displayed in each field to the right of the field name. Click on to exit the window.

Viewing and Configuring Link/Seg Traps for Hub Modules

To enable or disable Link and Segmentation traps for all ports on the selected hub module or modules:

1. In the Repeater Link/Seg Traps window, select a repeater interface in the scroll list.
2. Click mouse button 1 on ; the module traps window, [Figure 3-3](#), will appear.

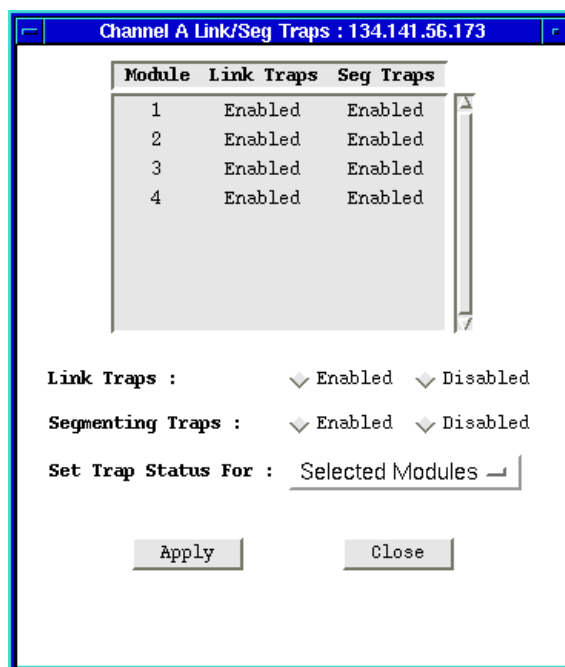


Figure 3-3. The Module Traps Window

- In the Module Traps window, click mouse button 1 to select the module for which you wish to configure link and segmentation traps. If the **Set Trap Status For** field displays *Selected Modules* (the default setting), you can click to select any modules; to de-select any highlighted module, click on it again. If the selection *All Modules* is displayed in the **Set Trap Status For** field, all available modules will be automatically selected; if you de-select any module, the **Set Trap Status For** field will automatically revert to the *Selected Modules* setting. To change the setting in the **Set Trap Status For** field, click mouse button 1 on the currently displayed setting, and drag down to select a new setting.
- Click on the appropriate selection in the **Link Traps** field to **Enable** or **Disable** link traps for the selected modules, as desired.
- Click on the appropriate selection in the **Segmenting Traps** field to **Enable** or **Disable** segmenting traps, as desired.
- Click on to save your changes; click on to exit the window.

Viewing and Configuring Link/Seg Traps for Ports

To enable or disable Link and Segmentation traps for individual ports:

- In the Repeater Link/Seg Traps window, select a repeater in the scroll list.

- Click mouse button 1 on ; the Port Traps window, Figure 3-4, will appear.

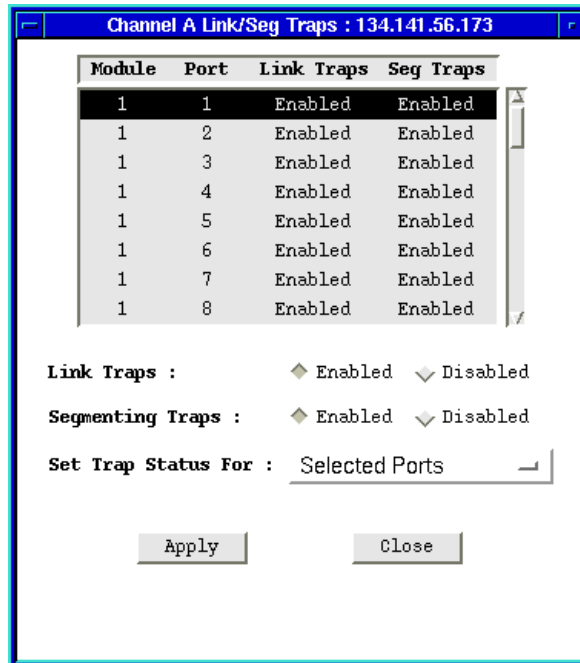


Figure 3-4. The Port Traps Window

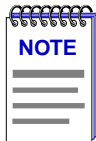
- In the port traps window, click mouse button 1 to select the port or ports for which you wish to configure traps. If the **Set Trap Status For** field displays *Selected Ports* (the default setting), you can click to select any ports; to de-select any highlighted port, click on it again. If the selection *All Ports on Module* is displayed in the **Set Trap Status For** field, you can select only one port at a time; trap status will be set for all ports on the same module as the selected port. If the selection *All Ports on Repeater* is displayed in the **Set Trap Status For** field, all available ports will be automatically selected; if you de-select any port, the **Set Trap Status For** field will automatically revert to the *Selected Ports* setting. To change the setting in the **Set Trap Status For** field, click on the currently displayed setting, and drag down to select a new setting.
- Click on the appropriate selection in the **Link Traps** field to **Enable** or **Disable** link traps for the selected modules, as desired.
- Click on the appropriate selection in the **Segmenting Traps** field to **Enable** or **Disable** segmenting traps, as desired.
- Click on to save your changes; click on to exit the window.

Repeater Redundancy

This chapter describes how to configure and enable redundant circuits.

Setting Network Circuit Redundancy

The redundancy application gives you the ability to define redundant circuits for your SEHI to ensure that critical network connections remain operational. Each circuit has a designated primary port and one or more backup ports. The SEHI monitors the link status of the primary port's connection to one or more network IP addresses; if the link fails, the SEHI automatically switches traffic to a backup port.



Before you configure redundancy, make sure that only the primary physical link is connected to the network. If a backup port is connected before you configure and enable redundancy, you create a data loop.

To open the main Repeater Redundancy window:

from the icon:

1. Click on the appropriate device icon to display the icon menu.
2. Drag down to **Redundancy** and release.

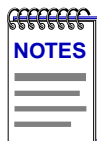
from the Hub View:

1. Click on to display the **Device** menu.
2. Drag down to **Redundancy** and release.

from the command line (stand-alone mode):

1. From the appropriate directory, type:

```
spmarun r4red <IP address> <community name>
```



The `spmarun` script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. The script is automatically invoked when you launch the application from the icon menu or from within the Hub View.

If you wish to change any redundancy settings, be sure to use a community name with at least Read/Write access. If you only wish to **view** current settings, a community name with Read access will be sufficient.

If there is a hostname mapped to your SEHI's IP address, you can use `<hostname>` in place of `<IP address>` to launch this application. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.

The main Repeater Redundancy window, [Figure 4-1](#), will appear.

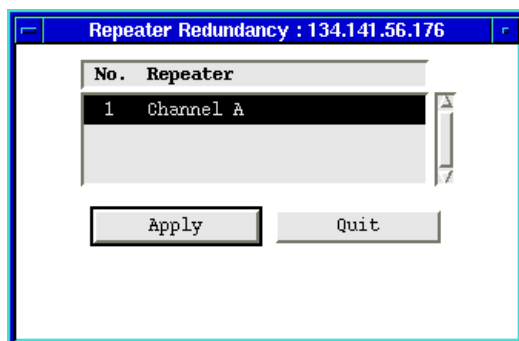


Figure 4-1. The Repeater Redundancy Window

Configuring a Redundant Circuit

To establish or edit a redundant circuit:

1. In the Repeater Redundancy window, click mouse button 1 on the repeater interface for which you would like to edit or establish a redundant circuit, then click . The Channel X Redundancy window, [Figure 4-2](#), will appear.

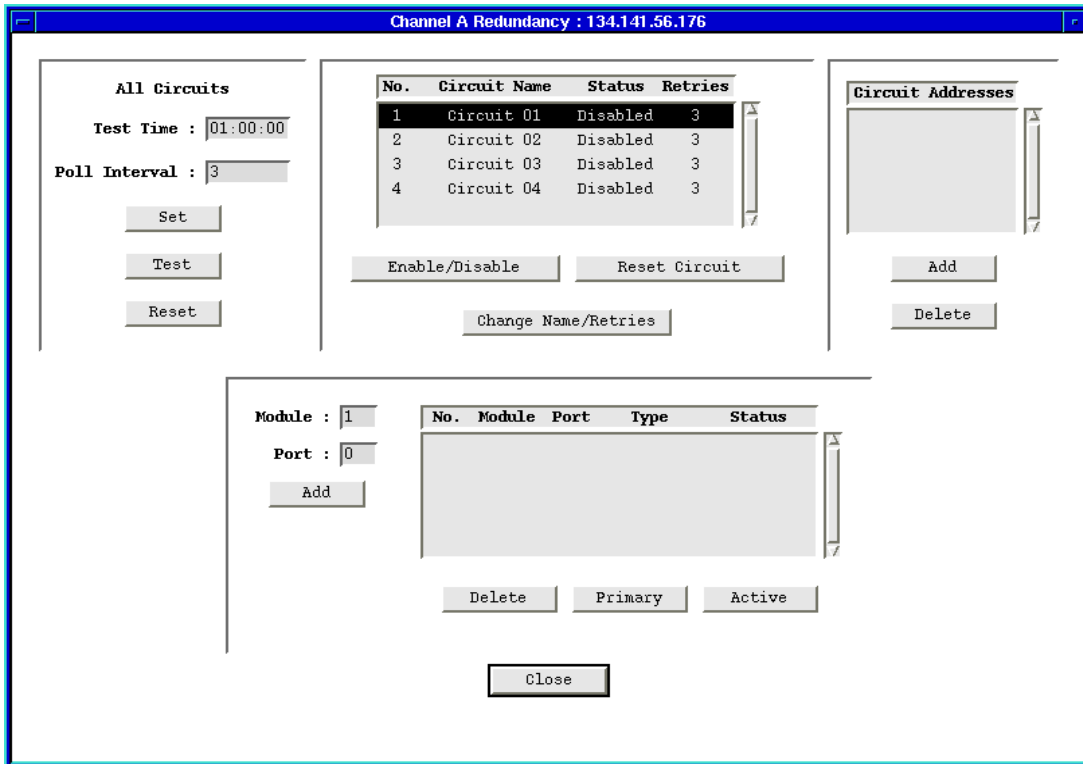


Figure 4-2. The Channel X Redundancy Window

2. If you want to change a circuit's name or the number of retries, highlight the appropriate circuit and click . The Change Circuit window, [Figure 4-3](#), will appear.

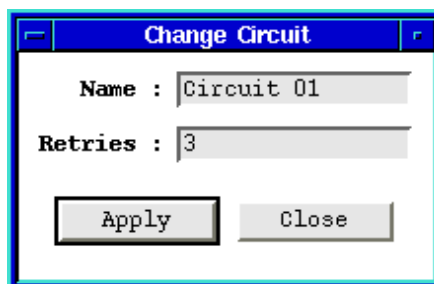


Figure 4-3. The Change Circuit Window

In the appropriate boxes, enter a new circuit name (up to 16 alphanumeric characters) and/or number of retries; **Retries** is the number of times the SEHI tests the connection to the first IP address listed in the Circuit Addresses window before it gives up and moves on to the next address. The valid range

of retries you can enter into this field is 0-16. Be sure to click on before exiting the window to save your changes.

3. With the appropriate Circuit Name highlighted, click to access the Add Circuit Address window, [Figure 4-4](#).

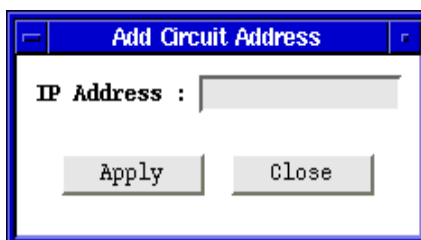
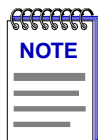


Figure 4-4. The Add Circuit Address Window

In this window you can define IP addresses of up to 8 devices on the network. These addresses identify the destination nodes that the SEHI looks for to determine the status of the active link. If the device determines that it has lost the link with the first address in the Circuit Addresses list, it checks the link status with the next address. If it can't establish a link with any address in the list, the device switches traffic to a backup port.

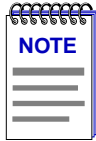
- a. To add a circuit address, enter a valid network IP address and then click . Repeat as necessary to add additional addresses. Click to exit the window.



The SEHI will poll the circuit addresses in the order they were entered.

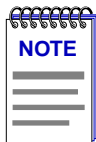
- b. To delete a circuit address, highlight the address in the Circuit Addresses list in the Channel X Redundancy window, and click .
4. The bottom half of the Channel X Redundancy window is where you define the primary port and backup ports for the highlighted Circuit Name. The **Status** of the Circuit Name must be set to **Disabled** when you configure the port list. Using the **Module** and **Port** boxes and the **Add** button, enter up to 8 ports to define the circuit.
 5. By default, all ports are created as **Inactive Backup** ports. You should set one port to be the Primary port and one port to be the Active port. Typically, the same port is both Primary and Active but this is not required. To select primary and active ports, click button 1 on a port to highlight it then click ; select the same or another port and click . Only one port can be the Primary port and only one port can be Active at any one time; if you set a

different port to be Primary or Active, the original Primary or Active port automatically resets to Backup/Inactive.



All backup ports will be disabled as soon as you enable the redundant circuit. The ports remain disabled until they become active due to primary port failure. If you disable the redundant circuit, you must manually enable each backup port in that circuit.

- Once you have configured all the ports that compose the redundant circuit, enable the circuit by clicking .

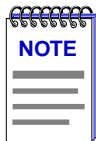


Be sure to make all physical connections to the backup ports once the redundant circuit has been configured and enabled.

To clear the settings in one circuit, highlight the Circuit Name that you want to clear, and click on .

To clear all redundancy configurations, click on in the All Circuits portion of the window. **Reset** does the following:

- Deletes all entries in the Circuit Addresses box
- Changes the status of every Circuit to Disabled
- Reverts to previous Circuit Name(s)
- Clears all module and port entries



After clearing redundancy settings by either method, backup ports remain disabled until you manually reenables them so that data loops do not occur. Before you enable the ports, disconnect their physical connections.

Monitoring Redundancy

Once you have configured your redundant circuits, you can use the fields in the All Circuits box to set the parameters that the SEHI uses to periodically test each of the circuits. The SEHI automatically polls all enabled circuits through the Primary port and all Backup ports at the time specified in the **Test Time** box. If the first poll fails (results in a no link condition with all of the circuit IP addresses), the SEHI checks the circuit's **Retries** field. If **Retries** is greater than 0, the SEHI waits the number of seconds specified in the **Poll Interval** field, and then polls the circuit again.

To set the **Poll Interval**:

1. In the All Circuits box, type in a new value in the **Poll Interval** field and click . Poll Interval is the time in seconds between retries (if the first attempt is unsuccessful).

To set the **Test Time**:

1. In the All Circuits box, type a new test time in the **Test Time** field in a 24-hour HH:MM:SS format and click . The Test Time is the time of day when the SEHI polls the addresses listed in each of the enabled circuits.

To immediately test all enabled circuits:

1. Click in the All Circuits box.

Source Addressing

Displaying the Source Address list; setting the Ageing Time; selecting the Hash Type; effects of Source Address Locking; configuring Source Address traps; finding a Source Address.

Displaying the Source Address List

The Source Address List, or Table (SAT), contains the MAC address and its associated vendor name for each device communicating through a port in the SEHI (or SEHI-controlled) hub. Each detected source address is also identified by the module and port through which it is communicating with the SEHI.

To view a SEHI's Source Address List:

from the icon:

1. Click on the appropriate device icon to display the icon menu.
2. Drag down to **Source Address** and release.

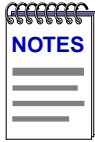
from the Hub View:

1. Click on to display the Device menu.
2. Drag down to **Source Addressing** and release.

from the command line (stand-alone mode):

1. From the appropriate directory, type

```
spmarun r4sa <IP address> <community name>
```



The *spmarun* script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.

If you wish to change any Source Address settings, be sure to use a **community name** with at least Read/Write access. If you only wish to view current settings, a community name with Read access will be sufficient. If you wish to lock or unlock ports, you must use a community name with SuperUser access.

If there is a hostname mapped to your SEHI's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.

The Repeater Source Address window, **Figure 5-1**, will appear.

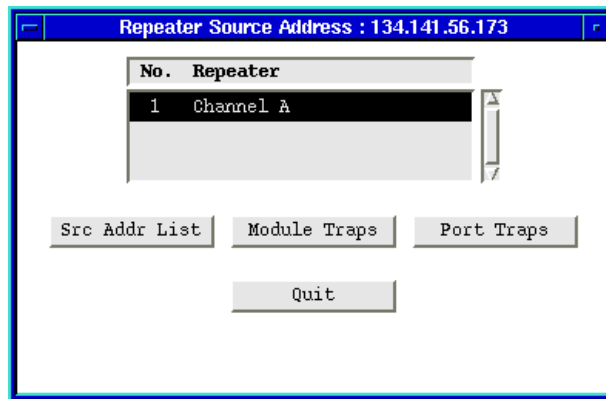


Figure 5-1. The Repeater Source Address Window

The Repeater Source Address window provides a list of the repeater interfaces available on the SEHI, as well as command buttons that allow you to display the Source Address List and enable and disable module and port source addressing traps.



The ability to enable or disable source addressing traps at the module and port level is not available in all versions of repeater device firmware; if the **Module Trap** and **Port Trap** buttons are grayed out, these features are not available on your device. Contact Cabletron Systems Technical Support for more information on upgrading your device firmware.

To view the source address list for the device, highlight the interface for which you wish to view the SAT, then click mouse button 1 on **Src Addr List**; the Source Address List window, **Figure 5-2**, will appear.

Channel A Source Address : 134.141.56.173

No.	Module	Port	MAC Address	Vendor
101	1	1	00:00:1D:0E:C6:B6	Cabletron
102	1	1	00:00:1D:11:C2:06	Cabletron
103	1	1	00:00:1D:02:0C:F5	Cabletron
104	1	1	00:00:1D:11:FC:71	Cabletron
105	1	1	00:00:1D:0F:FD:ED	Cabletron
106	1	1	00:00:1D:16:1C:42	Cabletron
107	1	1	00:00:1D:0C:AC:A8	Cabletron
108	1	1	00:00:1D:0F:6F:B8	Cabletron
109	1	1	00:00:1D:11:E7:5A	Cabletron
110	1	1	00:00:1D:18:D0:F7	Cabletron

Active Users : 313

Aging Time (minutes) : 60

Hash Type : nonDec Dec

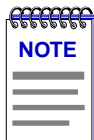
Source Address Lock : Lock Unlock

Source Address Traps : Enabled Enabled Disabled

Apply Find Refresh Close

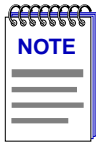
Figure 5-2. The Source Address List Window

The Source Address List window displays addresses of all devices that have transmitted packets through the SEHI within a time period less than the SAT's defined ageing time (addresses that have not transmitted a packet during one complete cycle of the ageing timer will be purged). The Ageing Time is user-configurable; see [Setting the Ageing Time, page 5-4](#). The list window can display about ten addresses at once; use the scroll bar to the right of the list window to view additional addresses, if necessary.



Some entries in the Source Address List window may list port numbers 25 or 26; port 25 represents EPIM 1, and port 26 represents EPIM 2.

Since the SAT is constantly changing as old entries are aged out and new ones learned from the network, you should occasionally update the displayed list by clicking mouse button 1 on Refresh. Once displayed, the list is static and will not reflect recent changes. Also static is the displayed number of **Active Users**; this field will also update when you click on Refresh.



The snapshots of the Source Address List that you can obtain via this feature do not reflect the current port security status of the SAT — that is, when Source Address Locking is enabled, you can still observe addresses being aged out of the table (for all ports) and new addresses being added (for trunk ports) as you refresh the Source Address List displayed in this window. However, the SEHI remembers the addresses that were in the table when locking was enabled, and will continue to protect station ports (and, in later versions of EMME/EMM-E6 firmware, RIC MIM trunk ports) from access by unauthorized sources. For more information, see [Locking Source Addresses](#), page 5-5.

Setting the Ageing Time

The source address list Ageing Time determines the *minimum* amount of time an inactive source address will remain in the Source Address Table before it is purged. The source address timer runs continuously beginning at the time the device is turned on; source addresses that are added to the SAT during one timer cycle will remain in the table for the rest of the current cycle and at least through the next complete cycle. If no packets have been received from that address during one complete cycle, the address will be purged.

The Ageing Time is user-configurable, and can be set using the **Ageing Time** text box in the Source Address list window.

To change the Ageing Time:

1. In the Source Address List window ([Figure 5-2](#), [page 5-3](#)), highlight the displayed ageing time.
2. Enter your desired ageing time in minutes; allowable range is 0 to 4320 (three days).
3. Click mouse button 1 on to save your change.

The new Ageing Time takes effect immediately.

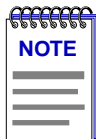
Setting the Hash Type

You can increase the efficiency with which your SEHI handles the Source Address Table by selecting the appropriate hashing algorithm. If you are operating in a DECnet environment, or one which incorporates some DECnet elements, select the DEC hashing algorithm; if your network contains no DECnet elements (or at least none operating on the same network segment as your SEHI), select the non-DEC hashing algorithm. Making the wrong selection won't do any damage, but making the correct selection will optimize performance.

To set the Hash Type for a repeater interface, or channel:

1. In the Repeater Source Address window, click mouse button 1 on the repeater interface for which you would like to set the hash type.

2. Click mouse button 1 on ; the Channel X Source Address List window, [Figure 5-2 \(page 5-3\)](#), will appear.
3. In the **Hash Type** field, click mouse button 1 on the appropriate selection to apply **Dec** or **nonDec** hashing to all ports on the selected repeater channel.
4. Click mouse button 1 on to save your changes; click on to exit the window.

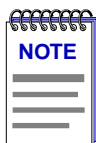


If your SEHI firmware does not support the Hash Type feature, this field will be unavailable.

Locking Source Addresses

When Source Address Locking is enabled, it puts into place a number of security measures designed to protect your Stack from unauthorized access. Depending on the revision of firmware installed on your SEHI and the kinds of Modules in the STACK, locking ports can provide a number of different protections, including secure address assignment, trunk port locking, configurable violation response, both eavesdrop and intruder protection, multi-level locking modes, and new definitions for station and trunk ports: station ports are those detecting zero, one, or *two* source addresses; trunk ports are those detecting *three* or more.

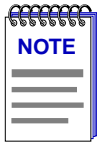
Enabling port locking from the Source Address List window activates all applicable security protections, as configured via the Security application (described in **Chapter 5** of this guide).



*Since the multi-level locking feature cannot be implemented from the Source Address List window, locking ports from this window will apply Full lock status by default to any ports which are currently unlocked. Any ports which are already in Continuous lock mode, however, will remain so. For more information on these lock modes and other security features, see Chapter 5, **Security**.*

To enable or disable Source Address Locking:

1. Click mouse button 1 on the appropriate option in the **Source Address Lock** field.
2. Click mouse button 1 on to set your new lock status.



Remember, you must have SuperUser (SU) access to the device in order to lock or unlock ports.

In addition to activating the security measures as configured via the Security application, locking source addresses has the following effects:

- On devices running older versions of firmware, unlinked ports will be disabled immediately after locking has been enabled; these ports can be re-enabled using their port menus, but they will immediately be disabled again if a device is connected and begins transmitting (since the port's source address table was locked in an empty state). On devices with newer firmware, unlinked ports are not automatically disabled in response to port locking, but they, too, will be immediately disabled if a device is connected and attempts to transmit packets.
- Although the Source Ageing Interval does not apply to station ports when Source Address Locking is enabled, the snapshot of the SAT provided by the Source Address List window may show a learned source address ageing out if that address remains inactive, and the appropriate trap will be generated.
- Once Source Address Locking has been enabled, each port's topology status (station or trunk) remains fixed and will not change while locking remains enabled, regardless of any changes in the number of source addresses detected.
- If Source Address Locking has been enabled, and one or more ports have been shut down because a new source address attempted access, those ports will remain disabled even after the SEHI has been reset, and must be re-enabled manually.

Source Address Locking on Older Devices

If your SEHI is running a firmware version previous to 1.05.01, Source Address Locking is implemented somewhat differently:

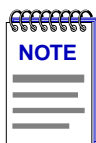
- Station ports are defined as those detecting zero or one source address; trunk ports as those detecting two or more.
- If a locked station port experiences a violation, the port will be automatically disabled and no traffic will be allowed through — not even traffic from the known source address.
- Trunk ports are never locked.
- Unlinked ports are immediately disabled.
- The Source Ageing Interval does not apply to locked station ports.

- A port's topology status (station or trunk) remains fixed while locking is in effect, even if the number of detected addresses changes.
- Any ports disabled due to a violation (or because they were unlinked when locking was enabled) must be manually re-enabled via their Port menus, and
- There are no additional Security features available.

If you are not sure which set of port locking features your device firmware supports, contact Cabletron Systems Technical Support.

Configuring Source Address Traps

The SEHI can issue several different traps in response to changes in the Source Address Table; you can enable and disable certain of these traps for the SEHI as a whole, and, if your device has very new firmware, they can also be enabled or disabled for each individual module and port.



*If the **Module Traps** and **Port Traps** buttons on the Repeater Source Address screen are grayed-out, your device firmware does NOT support the ability to enable and disable source addressing traps at the module and port levels. Contact Cabletron Systems Technical Support for information about upgrading your device firmware.*

*SPMA does not accept the trap messages; that task is left to your network management system. (See the appropriate network management system documentation for details about viewing trap messages.) When this utility is used in stand-alone mode, traps will either be ignored when they return to the workstation from which you are running SPMA for the SEHI, or they will turn up at another management workstation which has been configured to accept traps. Note also that, regardless of the configuration performed using this utility, NO traps will be sent by the device unless its trap table has been properly configured; see the SEHI hardware manual and/or the **Trap Table** chapter in the **SPMA Tools Guide** for more information.*

You can enable and disable the following Source Address traps:

- A **newSourceAddress** trap is generated when a station port — one receiving packets from zero, one, or two source addresses — receives a packet from a source address that is not currently in its source address table. Information included in this trap includes the board number, port number, and source address associated with the trap. Trunk ports — those receiving packets from three or more source addresses — will not issue newSourceAddress traps.
- A **sourceAddressTimeout** trap is issued anytime a source address is aged out of the Source Address Table due to inactivity. The trap's interesting information includes the board and port index, and the source address that timed out. (See [Setting the Ageing Time](#), page 5-4, for more information.)

Other traps that will be sent in response to changes in source addressing (even when the above traps have been disabled) include:

- **PortTypeChanged** traps are issued when a port's topology status changes from station to trunk, or vice versa. The interesting information includes the board and port index, and the port's new topology status.
- A **lockStatusChanged** trap is generated when the ports in the hub are locked or unlocked using the Source Address Lock option in the Source Address List window or by using the lock options in the Security application; the interesting information is the new lock status. (See [Locking Source Addresses, page 5-5](#), or Chapter 5, **Security**, for more information.)
- **PortSecurityViolation** and **portViolationReset** traps are sent in response to changes related to port locking; if ports are locked, the **portSecurityViolation** trap indicates that a new source address has attempted access on one of the ports, and the configured security actions are being taken; the interesting information is the board and port index, and the violating address. **PortViolationReset** traps are sent when management intervention has re-enabled a port or ports previously disabled in response to a port security violation; the interesting information is board and port index. Again, see [Locking Source Addresses, page 5-5](#), for more information.

Device-level Traps

The current status of the device-level source addressing traps is displayed in the **Source Address Traps** field in the Source Address List window ([Figure 5-2, page 5-3](#)).

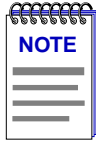
A status of **Enabled** indicates that source address traps have been enabled for *all* ports on *all* modules installed in the SEHI or SEHI-controlled hub; a status of **Disabled** indicates that source address traps have been disabled for *all* ports on *all* modules; and a status of **Other** indicates that there is some combination of enabled and disabled source address traps on the modules and/or ports in the hub or device.

To change the current status and enable or disable traps for all ports in the SEHI-controlled hub:

1. Click mouse button 1 on the appropriate option in the **Source Address Traps** field.
2. Click button 1 on to set your new trap status; the new status will be displayed to the left of the options in the **Source Address Traps** field. Note that enabling or disabling traps at the device level will eliminate any status of **Other** by setting all ports on all modules to the same status.

Module- and Port-level Traps

To set module- and port-level source addressing traps, select the appropriate channel in the Repeater Source Address window, then click on to enable and disable module-level traps, or on to enable and disable port-level traps.



It is not necessary to close the Source Address List before launching the module and port traps windows; just move the Source Address List window out of the way, if necessary, to reach the main Repeater Source Address window.

As with device-level trap status, a status of **Other** for any module indicates that there is some combination of enabled and disabled source address traps on the ports in that module.

To configure trap status for all ports on a selected module or modules:

1. In the Module Source Address Traps window (Figure 5-3, page 5-10), click mouse button 1 to select the module for which you wish to enable or disable traps. If the **Set Trap Status For** field displays *Selected Modules* (the default setting), you can click to select any modules; to de-select any highlighted module, click on it again. If the selection *All Modules* is displayed in the **Set Trap Status For** field, all available modules will be automatically selected; if you de-select any module, the **Set Trap Status For** field will automatically revert to the *Selected Modules* setting. To change the setting in the **Set Trap Status For** field, click mouse button 1 on the currently displayed setting, and drag down to select a new setting.
2. Click on the appropriate selection in the **Trap Status** field to enable or disable traps for the selected modules, as desired.
3. Click on to save your changes. Note that enabling or disabling traps at the module level will eliminate any module status of **Other** by setting all ports on the selected module or modules to the same status.

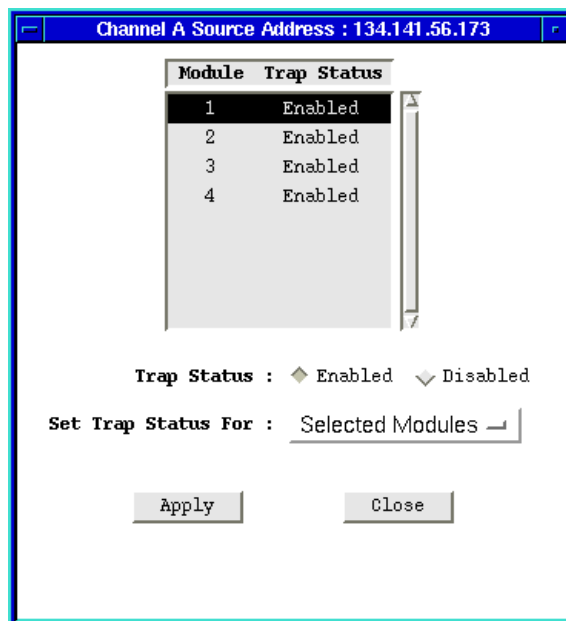


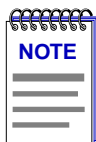
Figure 5-3. The Module Source Address Traps Window

To enable or disable port-level traps:

1. In the Port Source Address Traps window (Figure 5-4, page 5-11), click mouse button 1 to select the port or ports for which you wish to enable or disable traps. If the **Set Trap Status For** field displays *Selected Ports* (the default setting), you can click to select any ports; to de-select any highlighted port, click on it again. If the selection *All Ports On Module* is displayed in the **Set Traps Status For** field, you can select only one port at a time; trap status will be set for all ports on the same module as the selected port. If the selection *All Ports on Repeater* is displayed in the **Set Trap Status For** field, all available ports will be automatically selected; if you de-select any port, the **Set Trap Status For** field will automatically revert to the *Selected Ports* setting. To change the setting in the **Set Trap Status For** field, click mouse button 1 on the currently displayed setting, and drag down to select a new setting.

No.	MAC Address	Vendor
182	00:00:1D:03:2E:87	Cabletron
183	00:00:1D:0B:C2:C7	Cabletron
184	00:00:1D:05:6D:09	Cabletron
185	00:00:1D:08:98:25	Cabletron
186	00:00:1D:05:AA:C5	Cabletron
187	00:00:1D:05:62:AD	Cabletron
188	00:00:1D:09:59:D5	Cabletron
189	00:00:1D:0D:CC:B3	Cabletron
190	00:00:1D:07:9A:D0	Cabletron
191	00:00:1D:18:79:2A	Cabletron

Figure 5-4. The Port Source Address Traps Window

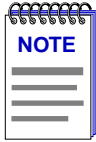


Some entries in the Port Source Address Traps window may list port numbers 25 or 26; port 25 represents EPIM 1, and port 26 represents EPIM 2.

2. Click on the appropriate selection in the **Trap Status** field to enable or disable traps for the selected port(s), as desired.
3. Click on to save your changes.

Finding a Source Address

You can use the button to locate a source address in the list by the module and port through which it is communicating with the SEHI. This feature is especially useful when your device is very busy and your source address table is quite large.



Note that each repeater channel maintains its own Source Address Table, and they are completely independent of one another; therefore, if you search for a source address communicating via Channel B from the Channel A Source Address List window, the result will be a “not found,” even though the address is connected to a port in the SEHI-controlled hub.

To find a source address:

1. Click mouse button 1 on in the Source Address List window (Figure 5-2, page 5-3); the Find Source Address window, Figure 5-5, will appear.

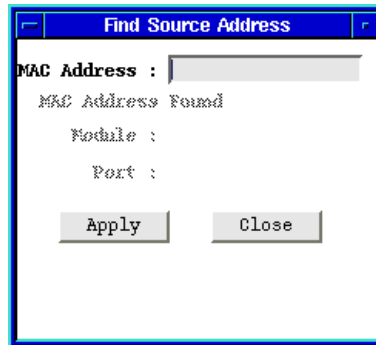


Figure 5-5. Find Source Address Window

2. In the **MAC Address** field, enter the source address you wish to locate in a hexadecimal (XX:XX:XX:XX:XX:XX) format.
3. Click on . If the address is in the table at the time the search is initiated, the remaining fields in the window will display the module and port through which the address is communicating with the SEHI. If the address is not in the table, the message **MAC Address Not Found** will display in the window. See Figure 5-6, page 5-13.

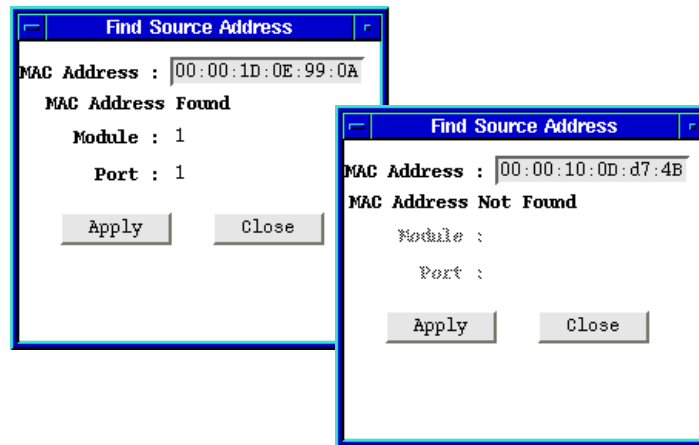


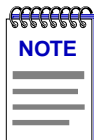
Figure 5-6. Results of MAC Address Search

4. Click on to exit the window.

Security

Launching the Security application; LANVIEWSECURE defined; configuring security; enabling security and traps at the repeater, hub, and port levels; security on non-LANVIEWSECURE Hubs

The Security application allows you to configure and manage the LANVIEWSECURE feature incorporated into the new generation of Cabletron's family of stackable hubs. LANVIEWSECURE provides enhanced intruder protection by allowing you to secure two source MAC addresses per port, along with an additional floating cache of up to 32 addresses among ports on a single hub; in addition, LANVIEWSECURE provides eavesdrop protection by scrambling the data portion of each packet to all ports except the destination port.



*Some portions of LANVIEWSECURE functionality will apply to **all** ports in the SEHI-managed hubstack, including ports residing on older, non-LANVIEWSECURE hubs; these will be noted throughout the text, and summarized in the section entitled **Security on Non-LANVIEWSECURE Hubs**.*

To launch the Security application

from the icon:

1. Click on the appropriate device icon to display the icon menu.
2. Drag down to **Security** and release.

from the Hub View:

1. Click on to display the Device menu.
2. Drag down to **Security** and release.

from the command line (stand-alone mode):

1. From the appropriate directory, type

```
spmarun r4sec <IP address> <SU community name>
```



The *spmarun* script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.

You must use a **community name** with Superuser access to run the Security application.

If there is a hostname mapped to your SEHI's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.

The Repeater Security window, [Figure 6-1](#), will appear.

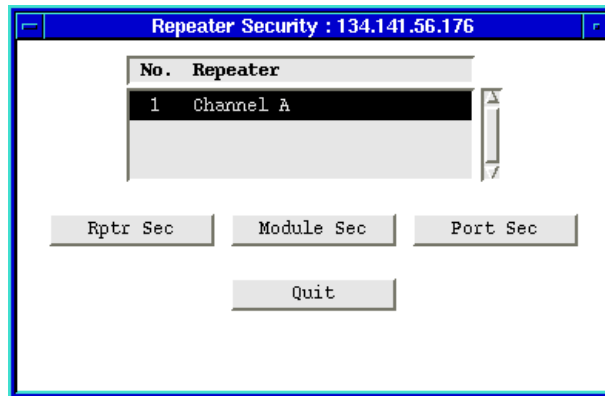


Figure 6-1. The Repeater Security Window

The Repeater Security window provides a list of the repeater interfaces available on the SEHI, as well as command buttons that allow you to configure security at the repeater, hub, and port levels.

What is LANVIEWSECURE?

LANVIEWSECURE comprises a set of enhanced security features that have been implemented on the new generation of Cabletron's stackable family (as designated by the letter "S" at the end of the hub name), and are supported by SEHI firmware versions 1.05.01 and above. When the LANVIEWSECURE feature is enabled, it provides two kinds of protection: *intruder protection* will prevent any unauthorized source addresses from communicating with the network via a

secure port, and can be configured to secure both station and trunk ports; *eavesdropper protection* scrambles the data portion of any packet transmitted via a secure port to all but the destination port, and can be extended to broadcast and multicast packets as well as packets destined for a single address. Security is activated by enabling port locking; you can lock and unlock ports and enable or disable traps at the repeater-, hub-, and port-level Security windows, as well as via the Source Address windows (see Chapter 4, **Source Addressing**, for more information).



When you lock ports from a repeater-, hub-, or port-level Security window, you have the option of setting two lock modes: Full or Continuous. When you lock ports via a Source Address window, the lock setting will default to the Full lock mode. See the section on Continuous Address Learning, below, or [Enabling Security and Traps](#), page 6-12 for more information on these two lock modes.

LANVIEWSECURE includes the following features:

New definitions for station and trunk ports

Under LANVIEWSECURE, station ports are now defined as those detecting zero, one, or *two* source addresses; trunk ports are defined as those detecting *three* or more.

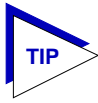
Secure address assignment

The first two source addresses detected on any port are automatically secured for both station and trunk ports; you can accept these default addresses as your secure addresses, or you can replace them. In addition, each hub contains a floating cache that allows you to assign an additional 32 secure addresses among the ports of your choosing.

Trunk port security

When locking is enabled, *all* ports will be secured — including natural trunk ports. (Only ports which have been forced to trunk status will remain unlocked.) Before implementing locking on trunk ports, however, be sure you have secured the necessary source addresses; as with station ports, only the first two detected source addresses are secured by default.

For devices with the newest security firmware (SEHI 1.10.xx and higher), a port's topology status — whether it is considered to be a station port or a trunk port — no longer determines its securability; securability is only determined by the number of source addresses in a port's source address table: any port which detects fewer than 35 source addresses will be locked. Ports which exceed those numbers are designated "unsecurable," and will be displayed as such in the port-level Security window; in addition, a new feature allows you to force any port to an unsecurable (that is, unlockable) state.



If your SEHI is running firmware more recent than 1.05.01 and previous to 2.10.xx, you will not have the ability to force a port to unsecurable status; however, for firmware versions in that range, ports which have been forced to trunk status will not be locked, so you can use the force trunk feature to render a port unsecurable if you wish.

Configurable violation response

Before *LANVIEW SECURE*, any locked port which experienced a violation was shut down automatically; now, you can choose to allow ports to remain enabled even after an unsecured address has attempted to access a locked port. If you choose **not** to disable a port which has experienced a violation, however, the port's only response to an intruder will be to issue a trap after the first violation; all packets, regardless of source address, will be allowed to pass. Ports in this state still have active eavesdropper protection (see definition below), and all packets addressed to any destination *other* than the secured address(es) will be scrambled.

Full or partial security against eavesdropping

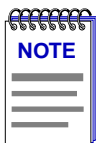
In addition to the enhanced intruder protection features described above, *LANVIEWSECURE* provides protection against eavesdroppers by scrambling the data portion of each packet to all ports *except* the port on which the destination address has been secured — in other words, the only port that will receive the packet in an unscrambled (readable) format is the port to which the packet was addressed. Two levels of eavesdropper protection are provided: full security scrambles all packets not specifically destined to the secured port, including broadcasts and multicasts; partial security scrambles only unicast packets.

The Newest *LANVIEWSECURE* Features

Additional *LANVIEWSECURE* features available on the newest firmware versions (SEHI 2.10.xx and higher) include:

Continuous learning mode

When configuring security on the newest *LANVIEWSECURE* devices, you can now choose between two levels of lock status: **Full** lock status, which behaves as locking has always done, and **Continuous** lock status, which essentially disables intruder protection by allowing the port to continue to learn new source addresses even when in a locked state. In this state, eavesdropper protection is still active, and will adjust so that packets addressed to the *current* learned address for a secured port are not scrambled.



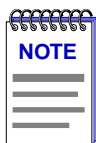
Locking ports from a Source Address window automatically provides Full lock status; however, locking ports from the repeater- or hub-level Source Address window does not override any existing Continuous lock status settings.

Forced non-secure status

With the original version of *LANVIEWSECURE*, all ports except those which had been forced to trunk status could be locked, and would be locked automatically if locking were enabled at the repeater or hub level. With the enhanced version of *LANVIEWSECURE*, this has changed in two ways: first, any port which has more than 35 addresses in its source address table (or exactly 35 addresses through two consecutive ageing times) is automatically considered **unsecurable** and cannot be locked while in this state; and second, you can force any port into this unsecurable state (as long as it is not already locked).

Learned addresses reset

By selecting the **Reset Learned Addresses** option in the repeater-, board-, or port-level Security window, you can clear all learned and secured addresses out of the selected port(s) address table, and allow that port to begin learning (and securing) new addresses. Note that you cannot reset learned addresses on a locked port or on a port which is designated unsecurable.



You cannot reset learned addresses or force non-secure status on a port which is already locked; in order to implement either of those features, you must first unlock the port.

Security on Non-*LANVIEWSECURE* Hubs

LANVIEWSECURE features as described above apply in total only to hubs designated as *LANVIEWSECURE* (as indicated by a label on the front panel and an “S” appended to the hub name). Some of the enhanced security features, however, will apply to all hubs installed in your SEHI-controlled hubstack, regardless of their *LANVIEW SECURE* status:

New definitions for station and trunk ports

All ports in your SEHI-controlled hubstack will be defined as station or trunk ports according to the new definitions: station ports are those detecting zero, one, or *two* source addresses; trunk ports are those detecting *three* or more.

Secure address assignment

Up to two source addresses detected on any *station* port are still automatically secured, and you can still accept or replace these default addresses. However, you cannot assign more than two secure addresses to any port (as there is no floating cache available), and neither natural nor forced trunk ports will ever be locked while in a trunk state.

Configurable violation response

You can still choose to allow ports to remain enabled even after an unsecured address has attempted to access a locked port. If you choose **not** to disable a port which has experienced a violation, however, the port’s only response to an

intruder will be to issue a trap after the first violation; all packets, regardless of source address, will be allowed to pass.

Forced non-secure status

With the enhanced version of *LANVIEWSECURE*, even ports on non-*LANVIEWSECURE* Hubs can be forced to an **unsecurable** status (as long as they are currently unlocked).

Learned addresses reset

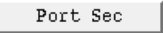
You can still use the **Reset Learned Addresses** option in the repeater-, board-, or port-level Security window to clear all learned and secured addresses out of the selected port(s) address table, and allow that port to begin learning (and securing) new addresses. Note that you cannot reset learned addresses on a locked port or on a port which is designated unsecurable.

Eavesdrop protection (scrambling), trunk port locking, continuous lock mode, and the floating address cache are not available for non-*LANVIEWSECURE* hubs.

Configuring Security

Most Security parameters are set via the port-level Security window; these will apply to the configured port regardless of the level at which security is enabled.

To access the Port Security window:

1. In the Repeater Security window, click to select the interface for which you would like to configure port-level security.
2. Click mouse button 1 on ; the Channel A Port Security window, [Figure 6-2](#), will appear.

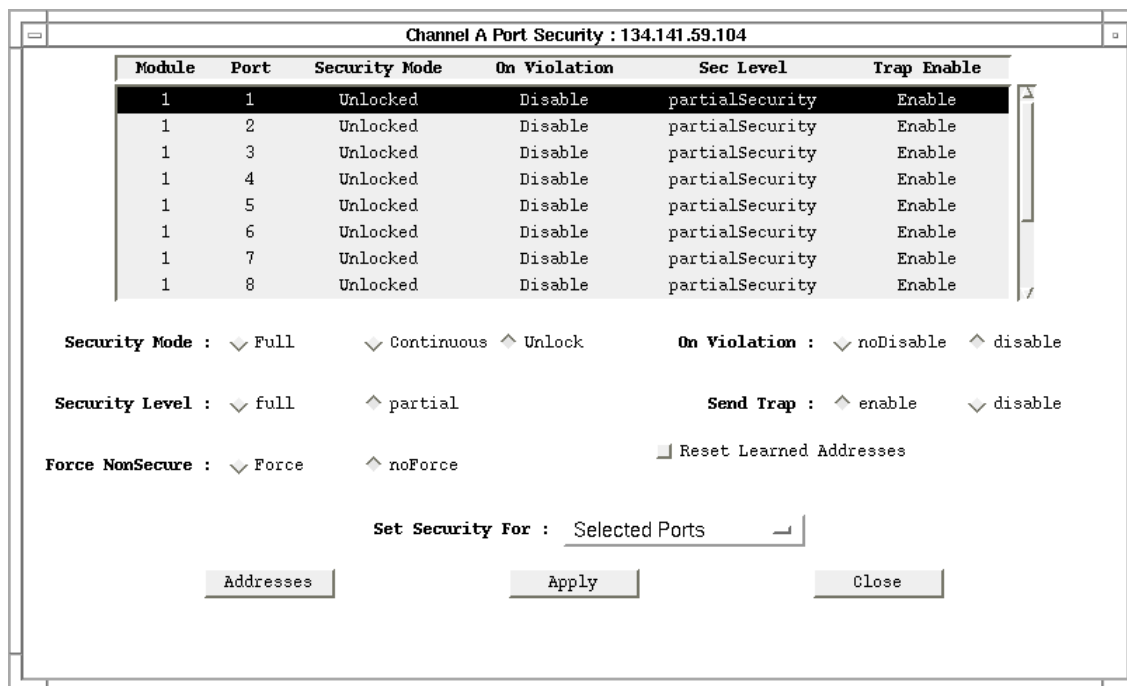


Figure 6-2. Channel A Port Security Window

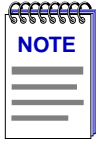
The top portion of the window contains a list box which displays each port communicating on the selected channel, designated by hub and port number. Each port's current Lock Status, violation response, Security Level, and Trap status is also displayed. Note that any ports on a non-LANVIEWSECURE hub will display "not applicable" in the Security Level field; eavesdropper protection (scrambling) and continuous lock mode cannot be implemented for these ports. (See [Security on Non-LANVIEWsecure Hubs](#), page 6-5, for more information.)

The lower portion of the window provides the fields you need to configure security for one or more of the listed ports. Note that if you select a group of ports with different security capabilities, only those capabilities which apply to every port in the selected group will be active; those which are not available for every port in the selected group will be grayed out.

To configure security levels and violation response:

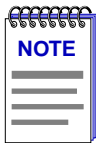
1. Use the **Set Security For** field or the mouse to select the port or ports for which you wish to configure security (note that the settings in the **Set Security For** field will change automatically as you click to select or de-select ports).
2. In the **On Violation** field, click to select **disable** if you want the port or ports to be disabled if any unauthorized source address is detected, or select **noDisable** if you wish the port to remain operational after a violation. Note that selecting the **noDisable** option effectively removes intruder protection

from the selected ports: a trap will be sent after the first violation, but all packets, regardless of source address, will be allowed to pass. Ports in this state still have active eavesdropper protection.



*Any ports which are disabled in response to a violation will remain disabled even after the SEHI has been reset, and must be re-enabled manually. See **Enabling /Disabling MIM Ports** in Chapter 2 for more information.*

3. The **Security Level** field allows you to select which packets not addressed to the selected ports will be scrambled: click to select **partial** if you wish to scramble the data portion of all packets *except* broadcasts and multicasts; select **full** if you wish to scramble broadcasts and multicasts as well. Note that scrambling can only be applied to *LANVIEWSECURE* hubs; this field will be grayed out if one or more non-*LANVIEWSECURE* hub ports has been selected in the list box.
4. Use the **Force NonSecure** field to designate which ports should be securable (that is, lockable) and which should be unsecurable. By definition, any *LANVIEWSECURE* port with more than 35 addresses in its source address table (or exactly 35 for two consecutive ageing times) is unsecurable, as are any non-*LANVIEWSECURE* ports with more than 3 addresses (or exactly 3 for two consecutive ageing times). Unsecurable ports — whether forced or natural — cannot be locked, and will be designated in the list box as **Unsecurable**.



You cannot force a port to Unsecurable status if it is already locked.

5. Click on to save your changes; the new Security Level and violation response settings will be displayed in the list box.

To assign secure addresses to a port:

1. Click to select a single port in the list box; the button will be activated.
2. Click on ; the Addresses window, [Figure 6-3](#), will appear.

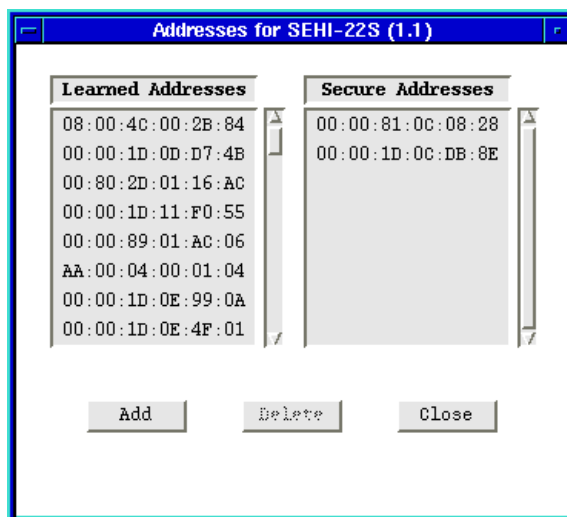
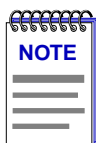


Figure 6-3. The Addresses Window

3. On the left side of the window, the **Learned Addresses** list box will display all source addresses detected by the selected port during the last ageing interval (see Chapter 4, **Source Address**, for more information on the ageing interval). On the right side of the window, the **Secure Addresses** list box will display the source addresses which have been secured for that port. Remember, as long as the port is in a securable state, the first two addresses detected by the port are automatically secured; you can add additional addresses, or delete the default addresses and secure new ones, as follows:
 - a. To add a learned address, click to highlight the desired address in the **Learned Addresses** list box, then click on . A confirmation window will appear; click on **Yes** to secure the selected address.



*If security has never been enabled, new addresses will **replace** any existing learned addresses. If security has ever been enabled — even if it is not currently enabled — new addresses will be stored **in addition to** any learned addresses.*

- b. To delete a secured address, click in the **Secure Addresses** list box to highlight the address you wish to delete, then click on . A confirmation window will appear; click on **Yes** to delete the address, or **No** to leave the address secured.
 - c. To add an address not yet detected by the port, make sure no Learned Addresses are highlighted, then click on ; the Add MAC Address window, [Figure 6-4](#), will appear.

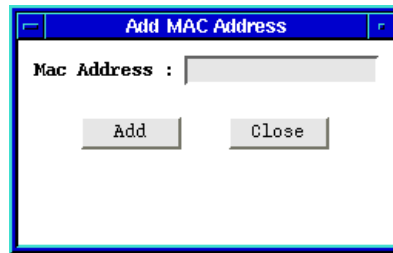
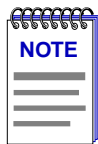


Figure 6-4. Add MAC Address Window

- d. Enter the desired MAC address in an xx:xx:xx:xx:xx:xx format, then click on . A confirmation window will appear; if you click on **Yes** to secure the address, it will appear in the **Secure Addresses** list box.
4. To secure addresses for additional ports, click to select the desired port in the Channel A Port Security window; the Addresses window will automatically display the Learned and Secure addresses for the new port.



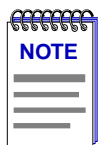
If the maximum number of addresses has already been assigned to the floating cache on the selected board, or if you have already secured two addresses on a non-LANVIEWSECURE hub port, the **Add** button will be disabled.

You can clear both Learned and Secure addresses (and re-start the learning process) by using the Reset Learned Addresses option in the repeater-, hub-, or port-level Security window; see [Resetting Learned Addresses, page 6-10](#).

Resetting Learned Addresses

You can clear all learned and secured addresses out of a port's address table, and allow that port to begin learning (and securing) new addresses, as follows:

1. In the Repeater Security window, click mouse button 1 on the repeater interface for which you would like to reset learned addresses.
2. Click mouse button 1 on , , or to open the appropriate window.
3. In the Module or Port window, click to select the hub(s) or port(s) for which you wish to reset learned addresses.



You cannot reset learned addresses for any port which is already locked or in an unsecurable state (either natural or forced). If you select a group of ports which includes one in a locked or unsecurable state, or if you select a hub or a repeater which has a port in one of these states, the Reset Learned Addresses option will be unavailable.

4. Click to select the **Reset Learned Addresses** option. A confirmation window will appear; click on to reset addresses, or on to cancel. The port's address table will be cleared of all Learned and Secure addresses, and the learning process will restart.

Tips for Successfully Implementing Eavesdropper Protection

There are a couple of things to note about eavesdropper protection, or scrambling, that must be taken into consideration as you are planning security for your network.

- Security can only be implemented by locking a port, and can only be completely disabled by unlocking the port. You cannot enable intruder protection on a *LANVIEWSECURE* hub without also enabling eavesdropper protection. You can, however, effectively enable eavesdropper protection alone by selecting the **noDisable** option for the violation response; selecting **noDisable** basically eliminates intruder protection, as all packets will be allowed to pass regardless of their source address. (Note, however, that the port will issue a trap after the first violation.) You can also enable eavesdropper protection without intruder protection by selecting the Continuous lock mode; see [Enabling Security and Traps, page 6-12](#), for details.
- Security must be disabled on any port which is connected to an *external* bridge, or the bridge will discard all packets it receives as error packets (since the CRC is not recalculated after a packet is scrambled).
- Security should also be disabled on any port which is supporting a trunk connection, unless you are sure that no more than 34 source addresses will attempt to use the port, and you have secured all necessary addresses. Note that, with the newest versions of security, a *LANVIEWSECURE* port that sees more than 35 addresses in its Source Address table (or exactly 35 addresses for two consecutive ageing intervals) is considered unsecurable and cannot be locked.
- Full security should not be implemented on any port which supports a Name Server or a BootP server, as those devices would not receive the broadcast and multicast messages they are designed to respond to (partial security — which does not scramble broadcasts or multicasts — will not affect their operation). Note that users who require responses to broadcast or multicast requests can still operate successfully if their ports are fully secured, as the *reply* to a broadcast has a single, specific destination address.

In general, scrambling is most effective when employed in a single hubstack which contains only *LANVIEWSECURE* hubs; remember, non-*LANVIEWSECURE* hubs do not support scrambling as part of their security functionality.

Enabling Security and Traps

You can enable or disable all applicable protections by locking or unlocking ports via the repeater, hub, or port Security window, as described in the sections below. There are two levels of lock status to choose from: if you select **Full** lock status, the port will stop learning new source addresses, accept packets only from secured source addresses, employ either full or partial eavesdrop protection (as configured), and take the configured steps (send trap and /or disable port) if a violation occurs; if you select **Continuous** lock status, the port will implement the configured level of eavesdrop protection, but continue to learn source addresses and allow all packets to pass, effectively disabling intruder protection.

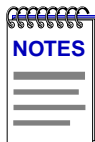
Enabling and disabling traps from the Security windows has the same effect as enabling and disabling them from the Source Address windows; you can enable and disable the following traps:

- A **newSourceAddress** trap is generated when a station port — one receiving packets from zero, one, or two source addresses — receives a packet from a source address that is not currently in its source address table. Information included in this trap includes the board number, port number, and source address associated with the trap. Trunk ports — those receiving packets from three or more source addresses — will not issue newSourceAddress traps.
- A **sourceAddressTimeout** trap is issued anytime a source address is aged out of the Source Address Table due to inactivity. The trap's interesting information includes the board and port index, and the source address that timed out. (See **Setting the Ageing Time** in Chapter 4, **Source Addressing**, for more information.)

All other source address traps (`portTypeChanged`, `lockStatusChanged`, `portSecurityViolation`, and `portViolationReset`, all defined in Chapter 4, **Source Addressing**) will continue to be generated as appropriate, as will the security-specific traps:

- A **secureStateChange** trap indicates that a port has changed from a securable state to an unsecurable state, or vice versa; the interesting information includes board and port index.
- A **learnStateChange** trap indicates that a port has had its learned addresses reset. Interesting information includes board and port index, and current learn state. Note that SPMA always maintains ports in a learn state, and just resets that learn state to achieve a reset of existing learned and secure addresses.
- A **learnModeChange** trap is issued when a port is set to continuous lock mode; interesting information includes board and port index, and current learn mode.

When setting these parameters at the various levels, keep in mind that the most recent setting will override the existing status: for example, if you lock one or more ports at the port level, then unlock them at the hub level, all ports on the hub will be unlocked. Similarly, if you enable traps at the hub level, then disable them at the repeater level, traps will be disabled for all ports on the repeater.

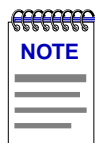


Enabling and disabling locking from the Source Address application (described in Chapter 4) will implement all applicable security features as they have been configured via the port-level Security window. Note that locking ports from the Source Address window implements **Full** lock status by default; however, this will not override the status of any ports which have already been set to **Continuous** lock mode.

Enabling and disabling traps from the Source Address window also has the same effect as enabling or disabling them from the Security application. Keep in mind, however, that SPMA does not accept the trap messages; that task is left to your network management system. (See the appropriate network management system documentation for details about viewing trap messages.) Note, too, that no traps will be sent by the SEHI unless its trap table has been properly configured; see the SEHI hardware manual and/or the **Trap Table** chapter in the **SPMA Tools Guide** for more information.

Repeater-level Security and Traps

Locking ports at the repeater, or channel, level applies all applicable security (as configured via the Port Security window) to every port on the channel.



If you select a repeater whose ports have different security capabilities, you may still be able to select and apply security states which are not applicable to all ports. Applying these kinds of settings will have no adverse affect on your network devices: those ports which can accept the set will do so; those which cannot will either ignore the set or issue a Set Failed.

To enable or disable security and traps for all ports on a repeater:

1. In the Repeater Security window, click mouse button 1 on the repeater interface for which you would like to configure port locking and/or traps.
2. Click mouse button 1 on ; the Channel A Security window, [Figure 6-5](#), will appear. Note that the current repeater-level settings are displayed immediately to the right of the field names; a repeater whose ports have different Security Mode or Trap settings will display a status of "Mismatch."

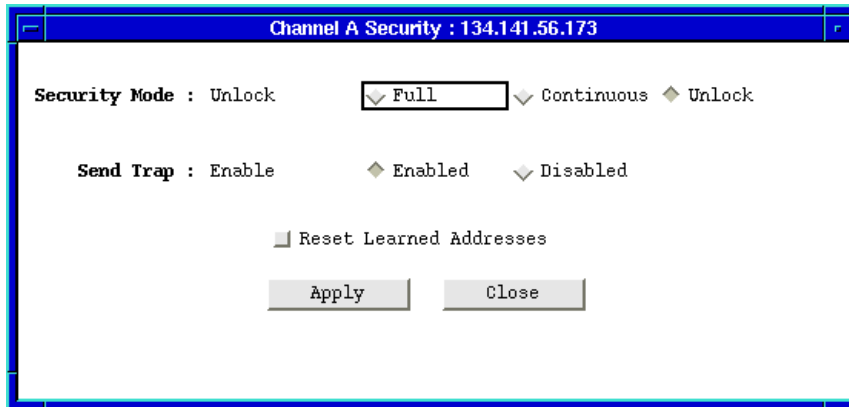
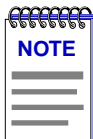


Figure 6-5. Channel A Security Window

3. In the **Security Mode** field, click mouse button 1 on the appropriate selection to apply **Full** or **Continuous** lock status to all ports on the selected repeater channel, or to **Unlock** all ports on the channel. (Note that if your SEHI does not support the newest security enhancements, the **Continuous** selection will be unavailable.)
4. In the **Send Trap** field, click mouse button 1 on the appropriate selection to **Enable** or **Disable** traps for the selected repeater channel.
5. Click mouse button 1 on to save your changes; the new status will be displayed in each field to the right of the field name. Click on to exit the window.

Hub-level Security and Traps

Locking ports at the hub level applies all applicable protections (as configured via the Port Security window) to each port on the selected hub or hubs.



If you select a group of hubs whose ports have different security capabilities, you may still be able to select and apply security states which are not applicable to all ports. Applying these kinds of settings will have no adverse affect on your network devices: those ports which can accept the set will do so; those which cannot will either ignore the set or issue a Set Failed.

To enable or disable locking and /or traps at the hub level:

1. In the Repeater Security window, click to select the appropriate repeater interface in the scroll list.
2. Click mouse button 1 on ; the Channel A Module Security window, [Figure 6-6](#), will appear. Note that the current hub-level settings are

displayed in the list box; a repeater whose ports have different Security Mode or Trap settings will display a status of “Mismatch.”

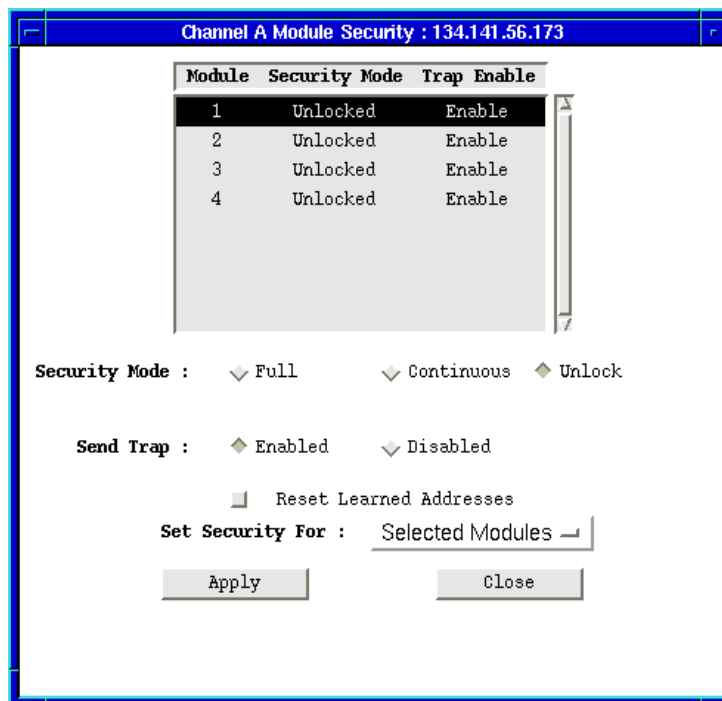


Figure 6-6. Channel A Module Security Window

- Use the **Set Security For** field or the mouse to select the hub or hubs for which you wish to configure security (note that the settings in the **Set Security For** field will change automatically as you click to select or de-select hubs).
- In the **Security Mode** field, click mouse button 1 on the appropriate selection to apply **Full** or **Continuous** lock status to all ports on the selected hubs, or to **Unlock** all ports on the hubs. (Note that if your SEHI does not support the newest security enhancements, the **Continuous** selection will be unavailable.)
- Click on the appropriate selection in the **Send Trap** field to **Enable** or **Disable** traps for the selected hub(s).
- Click on to save your changes; each hub's current status will be displayed in the scroll list. Click on to exit the window.

Port-level Security and Traps

To enable or disable security and/or traps at the port level:

1. In the Repeater Security window, click to selected the desired repeater interface, or channel, in the scroll list.
2. Click **Port Sec**; the Channel A Port Security window, [Figure 6-7](#), will appear.

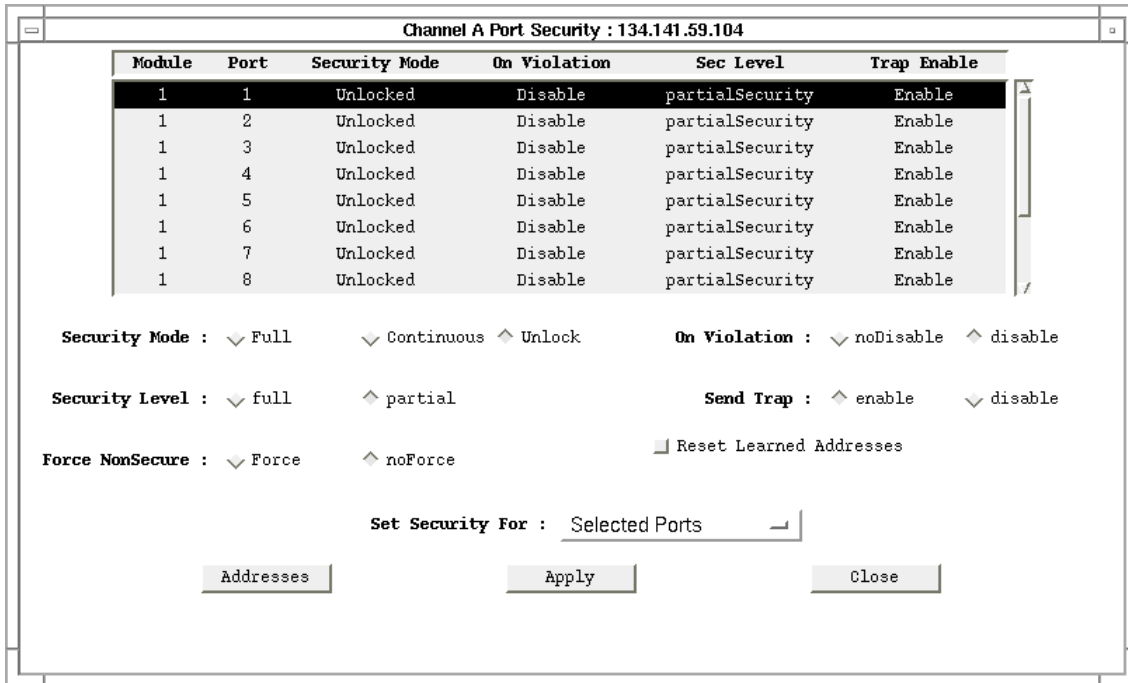
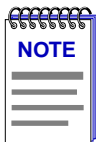


Figure 6-7. Channel A Port Security Window



For information on configuring security level, violation response, and secure addresses, see [Configuring Security, page 6-6](#). For information on resetting learned addresses, see [Resetting Learned Addresses, page 6-10](#).

3. Use the **Set Security For** field or the mouse to select the port or ports for which you wish to configure security (note that the settings in the **Set Security For** field will change automatically as you click to select or de-select ports).
4. In the **Security Mode** field, click mouse button 1 on the appropriate selection to apply **Full** or **Continuous** lock status to the selected port(s), or to **Unlock** selected ports. (Note that if your DEVICE does not support the newest security enhancements, or if the group of ports you have selected includes one on a non-LANVIEWSECURE hub, the **Continuous** selection will be unavailable.)

5. Click on the appropriate selection in the **Send Trap** field to **Enable** or **Disable** traps for the selected port(s).
6. Click on to save your changes; each port's new status will be displayed in the list box. Click on to close the window.

SEHI MIB Structure

SEHI management information base configuration

IETF MIB Support

In addition to its proprietary features, the SEHI-22/24 and SEHI-32/34 currently support the following IETF MIB:

- RFC 1213 MIB for Network Management of TCP/IP-based Internets: MIB-II

SEHI MIB Structure

Cabletron's newer intelligent devices — like the SEHI — organize MIB data into a series of "components." A MIB component is a logical grouping of MIB data, and each group controls a defined set of objects. For example, SEHI repeater information resides in its Repeater component; more generic device and port information resides in the SEHI Chassis MGR component.

The SEHI MIB consists of five components, each of which is described below. To see the names of the MIB components in your SEHI, bring up the Community Names application, or use any SNMP Get operation that will allow you to view the contents of the chCompTable.

The SEHI MIB consists of the following components:

SEHI Chassis MGR

The Chassis MGR MIB component contains most of the basic information about the SEHI, including: the SEHI's MIB component information (in the chCompTable), device names, hardware revision numbers, MAC and IP addresses, the current time and date, and information related to redundancy, alarms, and TFTP download. The system, interfaces, at, ip, icmp, udp, and snmp groups from MIB-II are also included. The community names assigned to this MIB component provide the gateway that all SPMA applications use to access all information in the other components, even if those components have different

community names; the Chassis MGR community names are the same as those assigned via Local Management.

SEHI LIM

The SEHI LIM, or Local Management, component contains the objects that provide out-of-band management via the Console port on the SEHI's front panel. No objects from this component are used for remote management.

Repeater One

The Repeater MIB component controls all repeater functionality on the SEHI. These functions include port count, port enable/disable, port status, board number, repeater statistics (packets, bytes, collisions, errors, etc.), protocol counts, and frame sizes; also included are the alarm, redundancy, source addressing, and trap functions. Note that the default community names for the Repeater MIB component will always be different from the default names assigned to all the other components.

SEHI Host Services

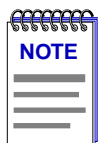
The Host Services MIB component contains the objects that provide the SEHI with its IP functionality — essentially, those functions which allow the SEHI to operate over a network — including functions such as ping, Telnet, and TFTP.

SEHI IP Services

The IP Services MIB component is not currently used by the SEHI, but is reserved for future use.

A Brief Word About MIB Components and Community Names

In the *original* version of the component MIB architecture, each MIB component is protected by its own set of user-configurable Read-Only, Read/Write, and Super-User community names. These names determine the level of access that will be granted to the information controlled by each individual component. For these devices, the central point of access for remote management is provided by the Chassis MGR MIB component — that is, if you define your device icon or launch a management application using the read-only, read/write, or super-user community name assigned to the Chassis MGR MIB component, your SPMA application is granted the appropriate level of access (read-only, read/write, or super-user) to all of that device's MIB information — even if the other MIB components have different community names (as will occur of necessity with the SEHI's multiple Network MIB components, each of which must have a unique set of community names).



The set of community names you assign via Local Management are those which apply to the Chassis MGR MIB component.

Newer versions of devices with this component-based MIB architecture have been simplified somewhat; these devices support a single, *global* set of community names, with small modifications added automatically to accommodate multiple instances of the same MIB component (as occurs with the SEHI's Network components). Again, defining your device icon or launching a management application with one of these global community names gives SPMA access to all MIB information.

Where community names may become an issue, however, is when you are using the MIBTree or any similar MIB-based tool (such as those provided by SunNet Manager or HP Network Node Manager) to access MIB information. For these kinds of tools, you must supply the *precise* community name assigned to the component that contains the information you want. For devices which support the original component-based MIB architecture, this means you must use the exact community name you have assigned to a specific component to access that component's MIB information. (Again, note that the SEHI's Network components always have *unique* community names.) For devices which support the new global community names, you must make note of the automatic modifications that are made for network components, and use those specific community names when trying to access information stored in those components.

The MIB component descriptions provided above will serve as a roadmap for determining where the information you're interested in is located; you can use the SPMA Community Names tool (described in **Chapter 3** of the *SPMA Tools Guide*) to determine whether your version of firmware supports the original component-based MIB architecture, or the new global community names. The Community Names tools also allows you to both view and set the community names which apply to your device.

A

- active port 4-4
- Active Users 2-12, 2-14, 2-20
- Add Circuit Address 4-4
- Admin Status 2-9
- Admin/Link Status 2-9
- Ageing Time 5-3, 5-4
- Ageing Timer 2-20
- Alignment Errors 2-17
- Avg Packet Size 2-16

B

- Broadcast Packets 2-16

C

- Change Name/Retries 4-3
- Charts and Meters 1-3
- Chassis MGR A-1
- Circuit Name 4-4
- Collisions 2-8, 2-17
- color codes 2-2, 2-6
- Community Names 1-3, 2-1, A-2
- component-based MIB architecture A-2
- connection status 2-6
- Contact 2-10
- Contact Status 2-2, 2-21
- continuous learning mode 6-4
- Continuous lock status 5-5
- conventions 1-3
- CRC Errors 2-17
- creating icons 1-3, 2-1
- Cyclic Redundancy Check (CRC) Errors 2-17

D

- Date 2-11
- default community names A-2
- Device button 2-4
- Device Configuration 2-22
- Device General Status 2-22
- Device menu 2-4, 2-7
- Device Name 2-3

- Device Status 2-10
- disable ports 2-22
- discovering Cabletron devices 1-3

E

- eavesdropper protection 6-3
 - tips for implementing 6-11
- enable ports 2-22
- Error Priority Scheme 2-18
- Errors 2-8

F

- FCS value 2-17
- find source address 5-12
- firmware version 1-7, 2-5
- floating address cache 6-3
- forced non-secure status 6-5, 6-6
- Frame Sizes 2-9, 2-19
- Front Panel 2-2, 2-22
- Full lock status 5-5

G

- General/Errors 2-16
- getting help 1-6
- Giant Frames 2-18
- global community names A-3

H

- help 1-6
- History window 1-4
- Host Services A-2
- hostname 2-1
- Hub View 2-1
- Hub View Front Panel 2-22
- hubstack 2-1

I

- icon menus, accessing 1-3
- IETF MIBs, supported by SEHI A-1
- inactive backup ports 4-4

Info window 2-5
intruder protection 6-2
IP Address 2-3
IP Services A-2

L

LANVIEWsecure 6-2
 on non-secure MIMs 6-5
learnModeChange trap 6-12
learnStateChange trap 6-12
LIM A-2
Link signal 2-6, 2-9
Link Status 2-13
link traps 3-1
Link/Seg Traps 2-4
Load 2-8
Local Management A-2
Location 2-3, 2-10
lock modes 6-3, 6-4
Locking Source Addresses 5-4, 5-5
lockStatusChanged trap 5-8

M

MAC Address 2-3, 5-1, 5-12
Media Type 2-14
MIB component A-1
MIB component descriptions A-3
MIB I, II 1-3
MIBTree 1-3
misaligned packets 2-17
Module menu 2-7
Module Traps 5-2, 5-7
Motif 1-3
Multicast Packets 2-17

N

Name 2-10, 2-13
newSourceAddress trap 5-7, 6-12

O

OOW Collisions 2-17
OSF/Motif 1-3

P

Poll Interval 4-5
polling intervals 2-4, 2-21
port color codes 2-6

Port Display Form 2-4, 2-8, 2-22
port display form
 options 2-8
port locking 5-5, 6-3
Port menu 2-7
Port Operational State 2-22
port security status 5-4
Port Source Address List 2-19
Port Status 2-13
Port Traps 5-2, 5-7
Port Type 2-9
portLinkDown 3-2
portLinkUp 3-2
PortSecurityViolation trap 5-8
portSegmenting 3-1
PortTypeChanged trap 5-8
portUnsegmenting 3-1
portViolationReset trap 5-8
primary port 4-4
Protocols 2-19
Protocols/Frames 2-16, 2-19

R

r4hwtr 3-3
r4red 4-2
r4sa 5-1
r4sec 6-2
receive collisions 2-17
Received Bytes 2-16
redundant circuits 4-1
Repeater One A-2
Reset Circuit 4-5
resetting learned addresses 6-5, 6-6, 6-10
Runt Frames 2-18

S

SAT 5-1
Save As Defaults 2-21
secure address assignment 6-3, 6-5
secure addresses 6-8
secureStateChange trap 6-12
Security 2-4, 5-5
security level 6-8
security parameters 6-6
security violation response 6-4, 6-5
segmentation traps 3-1
segmented 2-7, 2-9, 2-14
SEHI firmware 2-5
SEHI MIB components A-1

- Set Trap Status For 3-5, 3-6, 5-9, 5-10
- Setting Network Circuit Redundancy 4-1
- Source Address 2-4
- Source Address List 5-1
- source address locking 5-5
- Source Address Traps 5-8
- sourceAddressTimeout trap 5-7, 6-12
- spmarun 3-3, 5-1, 6-2
- stand-alone mode 1-3, 2-4
- Station 2-15
- station ports 5-5, 5-6, 6-3, 6-5
- Statistics 2-15, 2-22
 - general/errors 2-16
 - protocols/frames 2-16, 2-19
- Status 2-14

T

- Technical Support 1-6
- Test Time 4-5
- testing redundant circuits 4-5
- TFTP Download 1-3
- Time 2-11
- topology status 5-6
- Topology Type 2-15
- Total Errors 2-17
- Total Packets 2-16
- transmit collisions 2-17
- Trap Table 1-3
- Trunk 2-15
- trunk port security 6-3
- trunk ports 5-5, 5-6, 6-3, 6-5

U

- unique community names A-2
- unsecurable ports 6-3, 6-5, 6-6
- Uptime 2-3
- Use Defaults 2-21

V

- version numbers 1-6
- viewing trap messages 3-1, 5-7
 - stand-alone mode 3-1, 5-7

